# EL NUEVO PROTOCOLO DE INTERNET: IPv6

**PROYECTO DE GRADO**

**AURA MARIA RIVERA ARAGÓN**

**DIANA JANNETH ZULUAGA SOTO**

**UNIVERSIDAD TECNOLÓGICA DE PEREIRA**
**FACULTAD DE TECNOLOGÍA**
**PROGRAMA DE TECNOLOGÍA ELÉCTRICA**
**PEREIRA**
**2008**

# EL NUEVO PROTOCOLO DE INTERNET: IPv6

**AURA MARIA RIVERA ARAGÓN**

**DIANA JANNETH ZULUAGA SOTO**

**Trabajo de grado para optar por el título de**
**Tecnóloga en Electricidad**

**Profesor Guía**

**HUGO BALDOMIRO CANO GARZÓN**
**Especialista en Gerencia de Tecnología**

**UNIVERSIDAD TECNOLÓGICA DE PEREIRA**
**FACULTAD DE TECNOLOGÍA**
**PROGRAMA DE TECNOLOGÍA ELÉCTRICA**
**PEREIRA**
**2008**

## RESUMEN

El Protocolo de Internet versión 6 (Internet Protocol Version 6, IPv6) es el nivel más reciente del protocolo de Internet (IP) y actualmente se incluye como parte del soporte IP en muchos productos incluyendo los principales sistemas operativos de ordenador. El IPv6 ha sido llamado "IPng" (IP siguiente generación o Next Generation). Formalmente, el IPv6 es un grupo de especificaciones de la Fuerza de Tarea de Ingeniería de Internet (Internet Engineering Task Force, IETF).

El IPv6 se diseñó como un grupo de mejoras evolutivas a la actual versión 4 del IP Version 4. Los hosts de red y los nodos intermedios ya sea con IPv4 o IPv6 pueden manejar paquetes formateados para cualquier nivel del Protocolo Internet. Los usuarios y proveedores de servicio pueden actualizarse al IPv6 independientemente, sin tenerse que coordinarse entre sí. La más obvia mejora en el IPv6 sobre el IPv4 es que las direcciones IP se alargan de 32 a 128 bits. Esta extensión anticipa un considerable crecimiento futuro de Internet y proporciona un alivio a lo que se consideraba una inminente escasez de direcciones de red.

El IPv6 describe reglas para tres tipos de dirección: unicast (de un host a otro), anycast (de un host al más cercano de varios hosts), y multicast (de un host a múltiples hosts). Otras ventajas del IPv6 son:

- Se especifican opciones en una extensión al encabezado que sólo se examina en su destino, acelerando así el rendimiento general de la red.

- La introducción de una dirección "anycast" proporciona la posibilidad de enviar un mensaje al más cercano de varios hosts de puerta posibles con la idea de que cualquiera de ellos puede administrar el envío del paquete a otros. Los mensajes anycast pueden usarse para actualizar tablas de routing durante el proceso.

- Los paquetes pueden identificarse como pertenecientes a un "flujo" particular de modo que a los que son parte de una presentación de multimedia que tiene que llegar en "tiempo real" se les pueda proporcionar una mayor calidad de servicio (quality-of-service) comparados con otros clientes.

El encabezado IPv6 ahora incluye extensiones que permiten que un paquete especifique un mecanismo para autenticar su origen para asegurar la integridad de los datos y la intimidad.

Las diferencias más conocidas entre IPv4 y su predecesor, IPv6, radican en la posibilidad de tener un número extraordinariamente mayor de direcciones IP, así como en la optimización de su encabezado, lo que hace más eficiente la comunicación en todo el sistema de comunicaciones.

El nuevo protocolo IPv6 retiene la mayoría de los conceptos básicos de IPv4.
Al igual que IPv4, en IPv6 los data grama son no confiables y sin conexión. El formato de los data gramas en IPv6 es muy diferente al de IPv4. IPv6 provee nuevas funcionalidades como autentificación y seguridad. IPv6 organiza cada data grama como una secuencia de encabezados seguida de datos. Un data grama siempre comienza con un encabezado base de 40 octetos, el cual contiene las direcciones fuentes y destino y un identificador de flujo. El encabezado base puede estar seguido de 0 o más encabezados de extensión, seguido de datos. Los encabezados de extensión son opcionales; IPv6 los usa para codificar las mayoría a de las opciones de IPv4.

Desde tiempos atrás ya los sistemas operativos basados en UNIX, ya estaban implementando el protocolo IPv6 de forma experimental. IPv6 resuelve los problemas asociados con el diseño original del IPv4 y añade una serie de funciones que permiten, entre otras cosas, dar continuidad al gran crecimiento de Internet.

Este documento describe los problemas con que se encuentra IPv4 y cómo se resuelven con IPv6, el modelo de direccionamiento de IPv6, la nueva cabecera IPv6 y sus extensiones, la sustitución que se hace en IPv6 de los procotolos ICMP (Internet Control Message Protocol) e IGMP (Internet Group Management Protocol), interacción entre nodos próximos, y la autoconfiguración de direcciones con IPv6. Este documento también describe los conceptos fundamentales de IPv6 y está dirigido a los ingenieros y profesionales que estén familiarizados con los conceptos básicos de redes y TCP/IP.

# INTRODUCCIÓN

Internet está entre nosotros desde hace casi 30 años, pero sol durante los últimos diez años hemos empezado a considerarla como una herramienta indispensable en nuestra vida. Hoy ha llegado a ser la portadora de información, la suministradora de servicios básicos de los que todos dependemos, tales como el correo electrónico, los datos de voz y las previsiones de Web, además de proporcionar una infraestructura esencial para la comunicación industrial. El estándar generalizado hoy en día para la transmisión de datos en Internet se conoce como Protocolo de Internet Versión 4, o IPv4. Ya con una antigüedad de 20 años, el protocolo IPv4 ha demostrado tener una gran flexibilidad. Su estructura ha hecho posible que nuevos protocolos operen conjuntamente con él para suministrar servicios tales como soporte para tareas críticas en el tiempo, capacidad para dirigirse a personas en movimiento y aseguramiento de la comunicación, tareas para las cuales, en realidad, no se había diseñado Internet.
Pero el tiempo no pasa en balde: el cambio de las pautas de comportamiento de los usuarios y el aumento del tráfico están imponiendo nuevos requisitos a Internet.

IPv6 es una nueva versión del protocolo de Internet (IP) que ha sido diseñada como paso evolutivo de IPv4, la versión del protocolo de Internet en uso hoy en día.
El protocolo Ipv6, que puede instalarse como una mejora normal de software en dispositivos conectados a Internet, puede interoperar con IPv4. Los usuarios podrán mejorar sus ordenadores centrales instalando IPv6 y los operadores de redes podrán desplegarlo en los encaminadores con una mínima coordinación entre ellos.

IPV6 resuelve diversos problemas que se están produciendo con IPv4, tales como la limitación del número de direcciones disponibles, y ofrece mejoras en áreas tales como el encaminado y la configuración de redes. Se espera que el protocolo IPv6 vaya sustituyendo gradualmente al IPv4, aunque ambos coexistirán durante varios años en un periodo de transición. Se está desarrollando la implantación del protocolo IPv6 para muchos encaminadores y sistemas operativos de ordenadores centrales.

Muchas aplicaciones normales de Internet ya funcionan con IPv6, muchas otras están empezando a hacerlo…

# OBJETIVOS

## OBJETIVO ESPECÍFICO

Desarrollar una descripción bibliográfica que nos muestre y especifique los detalles más importantes de la nueva versión de El Protocolo de Internet: IPv6

## OBJETIVOS GENERALES

- ✓ Profundizar en el conocimiento del Protocolo IPv6.
- ✓ Desarrollar la teoría suficiente para implementar el Protocolo de Internet IPv6 en una red de datos.
- ✓ Documentar bibliográficamente el Protocolo de Internet IPv6.
- ✓ Comparar el Protocolo IPv4 con el Protocolo IPv6.

Nota de aceptación

_____

_____

_____

_____
Presidente del Jurado

_____
Jurado

_____
Jurado

## LISTA DE FIGURAS

## LISTA DE ANEXOS

**Pág.**

## AGRADECIMIENTOS

Al ingeniero Hugo Baldomiro Cano Garzón por ser nuestro guía y asesorarnos en el desarrollo de este trabajo.

Al ingeniero Edison Duque por su colaboración y disponibilidad en la realización y calificación de este proyecto.

A nuestras familias, les agradecemos su apoyo y fortaleza espiritual que nos proporcionaron.

# GLOSARIO

**6OVER4**
Una tecnología IPv6 diseñada para favorecer la coexistencia con IPv4, que proporciona conectividad unicast y multicast a través de una infraestructura IPv4 con soporte para multicast, empleando la red IPv4 como un enlace lógico multicast.

**6TO4**
Una tecnología IPv6 diseñada para favorecer la coexistencia con IPv4, que proporciona conectividad unicast entre redes y máquinas IPv6 a través de una infraestructura IPv4. 6to4 utiliza una dirección pública IPv4 para construir un prefijo global IPv6.

**ÁMBITO (SCOPE)**
Para las direcciones IPv6, el ámbito es la porción de la red a la que se supone que se va a propagar el tráfico.

**ANUNCIO DE ROUTERS**
Mensaje de descubrimiento de vecinos enviado por un router bien de forma pseudo-periódica o como respuesta a un mensaje de solicitud de router. El anuncio incluye al menos información acerca de un prefijo que será el que luego utilice el host para calcular su dirección IPv6 unicast según el mecanismo “stateless”.

**ARQUITECTURA DE PILA DUAL**
Una arquitectura para nodos IPv6/IPv4 en la que existen dos implementaciones completas de la pila de protocolos, una para IPv4 y otra para IPv6, cada una de ellas con su propia implementación de la capa de transporte (TCP y UDP).

**AUTOCONFIGURACIÓN DE DIRECCIONES**
Proceso de configuración automática de direcciones IPv6 en un interfaz.

**BUCLE DE ENCAMINADO**
Situación indeseable en una red, que provoca que el tráfico se retransmita siguiendo un bucle cerrado, con lo cual nunca llega a su destino.

**BIT**
Acrónimo de Binary digit. (Dígito binario). Un bit es un dígito del sistema de numeración binario. Mientras que en nuestro sistema de numeración decimal se usan diez dígitos, en el binario se usan solo dos dígitos, el 0 y el 1. Un bit o dígito binario puede representar uno de esos dos valores, 0 ó 1.

El bit es la unidad mínima de información empleada en informática, en cualquier dispositivo digital, o en la teoría de la información.

**BYTE**
Unidad básica de almacenamiento de información, generalmente equivalente a ocho bits, pero el tamaño del byte depende del código de caracteres o código de información en el que se defina.

Los prefijos kilo, mega, giga, etc. se consideran potencias de 1024 en lugar de potencias de 1000. Esto es así porque 1024 es la potencia de 2 (210) más cercana a 1000. Se utiliza una potencia de dos porque trabajamos en un sistema binario. Sin embargo, para el SI, los prefijos mantienen su significado usual de potencias de mil.

**BUCLE DE ENCAMINADO**
Situación indeseable en una red, que provoca que el tráfico se retransmita siguiendo un bucle cerrado, con lo cual nunca llega a su destino.

**CACHE DE ROUTERS**
Ver caché de destinos.

**CACHÉ DE DESTINOS**
Tabla mantenida por cada nodo IPv6 que mapea cada dirección (o rango de direcciones) destino con la dirección del siguiente router al que hay que enviar el datagrama. Además almacena la MTU de la ruta asociada.

**CACHÉ DE VECINOS**
Es una caché mantenida por cada nodo IPv6 que almacena la dirección IP de sus vecinos en el enlace, sus correspondientes direcciones de nivel de enlace, y una indicación de su estado de accesibilidad. Las caché de vecinos es equivalente a la caché ARP en IPv4.

**CHECKSUM DE LA CAPA SUPERIOR**
Cálculo del checksum realizado en ICMPv6, TCP y UDP que utiliza la pseudo-cabecera IPv6.

**CONTROL DE ACCESO AL MEDIO**
Es un subnivel del nivel de enlace de datos ISO definido por el IEEE. Sus funciones son la creación de tramas y la gestión del acceso al medio.

**DATAGRAMA**
Fragmento de paquete de datos que es enviado con la suficiente información como para que la red pueda simplemente encaminar el fragmento hacia el

ordenador receptor, de manera independiente a los fragmentos restantes. Esto puede provocar una recomposición desordenada o incompleta del paquete en el ordenador destino. La estructura de un datagrama es: cabecera y datos.

**DHCP (DYNAMIC HOST CONFIGURATION PROTOCOL)**
Un protocolo de configuración con estado ("stateful") que proporciona direcciones IP y otros parámetros de configuración para conexión a una red IP.

**DIRECCIÓN**
Identificador asignado a nivel de la capa de red a un interfaz o conjunto de interfaces que puede ser empleado como campo de origen o destino en datagramas IPv6.

**DIRECCIÓN 6OVER4**
Una dirección del tipo [prefijo 64-bit]:0:0:WWXX:YYZZ, en la que WWXX:YYZZ es la representación hexadecimal de w.x.y.z (una dirección publica o privada IPv4), empleada para representar una máquina en la tecnología 6over4.

**DIRECCIÓN 6TO4**
Una dirección del tipo [prefijo 64-bit]:0:0:WWXX:YYZZ, en la que WWXX:YYZZ es la representación hexadecimal de w.x.y.z (una dirección publica o privada IPv4), empleada para representar una máquina en la tecnología 6over4. Una dirección del tipo 2002:WWXX:YYZZ:[SLA ID]:[Interfaz ID], en la que WWXX:YYZZ es la representación hexadecimal de w.x.y.z (una dirección publica IPv4), empleada para representar un nodo en la tecnología 6to4.

**DIRECCIONES DE COMPATIBILIDAD**
Direcciones IPv6 que son empleadas al enviar tráfico IPv6 sobre una infraestructura IPv4. Ejemplos de direcciones de compatibilidad son: las direcciones compatibles-IPv4, las direcciones 6to4 y las direcciones ISATAP.

**DIRECCIONES IP**
Número que identifica a una interfaz de un dispositivo (habitualmente un ordenador) dentro de una red que utilice el protocolo IP.

Es habitual que un usuario que se conecta desde su hogar tenga una dirección IP asignada por el proveedor del servicio que cambia cada vez que se conecta; eso es una dirección IP dinámica (normalmente se abrevia como IP dinámica).

Los sitios de Internet que están permanentemente conectados generalmente tienen una dirección IP fija, es decir, no cambia con el tiempo y esto facilita la resolución de nombres con el Servicio DNS.

**DIRECCIÓN IPv4 MAPEADA**
Es una dirección de la forma 0:0:0:0:0:FFFF:w.x.y.z o ::FFFF:w.x.y.z, donde w.x.y.z es una dirección IPv4. Las direcciones IPv4 mapeadas se emplean para representar un nodo con soporte sólo IPv4 ante un nodo IPv6.

**DIRECCIÓN ISATAP**
Es una dirección del tipo [prefijo de 64-bit]:0:5EFE:w.x.y.z, siendo w.x.y.z una dirección IPv4, pública o privada, que se asigna a un equipo ISATAP.

**DNS**
(Domain Name System) Base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet. Aunque como base de datos el DNS es capaz de asociar distintos tipos de información a cada nombre, los usos más comunes son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico de cada dominio.

**DOMINIO**
Un dominio es la parte de una URL (dirección de una página o recurso en Internet) por la que se identifica al servidor en el que se aloja.

Es cada nodo que desciende del dominio raíz ".", y representa a una subred nominal (clasificada por nombres, diferente de una subred protocolar clasificada por direcciones IP) dentro del Sistema de Nombres de Dominio.

**ENCAPSULADO DE SEGURIDAD ESP (ENCAPSULATING SECURITY PAYLOAD)**
Una cabecera y cola de extensión IPv6 que proporciona autenticación del origen de datos, integridad y confidencialidad de datos y servicio anti-repetición para la carga del datagrama encapsulado por la cabecera y cola.

**ENLACE**
Uno o más segmentos de una red de área local limitados por routers.

**ESTADO DEL ENLACE**
Tecnología de protocolo de rutado, que intercambia información de rutas, que consta de los prefijos de las redes conectadas a un router y su coste asociado. La información del estado del enlace se anuncia en el arranque, así como cuando se detectan cambios en la topología de la red.

**ESTANDAR**
Especificación que regula la realización de ciertos procesos o la fabricación de componentes para garantizar la interoperabilidad.

**ETHERNET**
Nombre de una tecnología de redes de computadoras de área local (LAN) basada en tramas de datos. El nombre viene del concepto físico de ether. Ethernet define las características de cableado y señalización de nivel físico y los formatos de trama del nivel de enlace de datos del modelo OSI.

**EUI (EXTENDED UNIQUE IDENTIFIER)**
Dirección del nivel de enlace definida por el IEEE (Institute of Electrical and Electronic Engineers).

**FLUJO**
Una serie de datagramas intercambiados entre una fuente y un destino que requieren un tratamiento especial en los routers intermedios, y definidos por una dirección IP origen y destino específico, así como por una etiqueta de flujo con un valor distinto de 0.

**FRAGMENTACIÓN**
Proceso por el que se divide la carga de un datagrama IPv6 en fragmentos por la máquina emisora de modo que todos los fragmentos tienen una MTU apropiada al camino a seguir hasta el destino.

**FRAGMENTO**
Una porción de una carga enviada en un datagrama IPv6 enviada por un host. Los fragmentos contienen una cabecera de fragmentación.

**HOST**
Máquina conectada a una red de ordenadores y que tiene un nombre de equipo (en inglés, hostname); es un nombre único que se le da a un dispositivo conectado a una red informática. Puede ser un ordenador, un servidor de archivos, un dispositivo de almacenamiento por red, una máquina de fax, impresora, etc. Este nombre ayuda al administrador de la red a identificar las máquinas sin tener que memorizar una dirección IP para cada una de ellas que lo identifica.
También se llama así al dominio del equipo.

**IANA**
Acrónimo de Internet Assigned Number Authority. La Agencia de Asignación de Números Internet era el antiguo registro central de los protocolos Internet, como puertos, números de protocolo y empresa, opciones y códigos. Fue sustituido en 1998 por ICANN.

**ICMPV6 (INTERNET CONTROL MESSAGE PROTOCOL FOR IPv6)**
Protocolo para los mensajes de control de Internet para IPv6. Un protocolo que proporciona mensajes de error para el rutado y entrega de datagramas IPv6 y

mensajes de información para diagnóstico, descubrimiento de vecinos, descubrimiento de receptores multicast y movilidad IPv6.

**IDENTIFICADOR DE AGREGACIÓN DE MÁXIMO NIVEL**
TLA ID (Top-Level Aggregation Identifier). Campo de 13 bits dentro de la dirección unicast global reservada para grandes organizaciones o ISP por el IANA, y que por tanto identifica el rango de direcciones que tienen delegado.

**IDENTIFICADOR DE AGREGACIÓN DE SIGUIENTE NIVEL**
NLA ID (Next-Level Aggregation Identifier). Es un campo de 24 bits en la dirección unicast global agregable que permite a los ISPs crear varios niveles jerárquicos de direccionamiento en sus redes para organizar las direcciones y el rutado hacia otros ISPs, así como para identificar los sitios de la organización.

**IDENTIFICADOR DE AGREGACIÓN DE SITIO**
SLA ID (Site-Level Aggregation Identifier). Campo de 16 bits dentro de la dirección global unicast que utiliza una organización para identificar subredes dentro de su red.

**IEEE**
Corresponde a las siglas de The Institute of Electrical and Electronics Engineers, el Instituto de Ingenieros Eléctricos y Electrónicos, una asociación técnico-profesional mundial dedicada a la estandarización, entre otras cosas. Es la mayor asociación internacional sin fines de lucro formada por profesionales de las nuevas tecnologías, como Ingenieros de telecomunicaciones, Ingenieros electrónicos, Ingenieros en informática.

**INTERFAZ**
Una representación de un nexo físico o lógico de un nodo a un enlace. Un ejemplo de un interfaz físico es un interfaz de red. Un ejemplo de un interfaz lógico es un interfaz de túnel.

**INTERFAZ LOCAL**
Interfaz interna que permite que un nodo se envíe paquetes a sí mismo.

**INTERNET**
Interconexión de redes informáticas que permite a los ordenadores o computadoras conectadas comunicarse directamente, es decir, cada ordenador de la red puede conectarse a cualquier otro ordenador de la red. El término suele referirse a una interconexión en particular, de carácter planetario y abierto al público, que conecta redes informáticas de organismos oficiales, educativos y empresariales. También existen sistemas de redes más pequeños llamados

intranets, generalmente para el uso de una única organización, que obedecen a la misma filosofía de interconexión.

**IP (PROTOCOLO DE INTERNET)**

Cada computador que se conecta a Internet se identifica por medio de una dirección IP. Ésta se compone de 4 campos comprendidos entre el 0 y el 255 y separados por puntos.

No está permitido que coexistan en la Red dos computadores distintos con la misma dirección, puesto que de ser así, la información solicitada por uno de los computadores no sabría a cual de ellos dirigirse.

Dicha dirección es un número de 32 bit y normalmente suele representarse como cuatro cifras de 8 bit separadas por puntos.

La dirección de Internet (IP Address) se utiliza para identificar tanto al computador en concreto como la red a la que pertenece, de manera que sea posible distinguir a los computadores que se encuentran conectados a una misma red.

Con este propósito, y teniendo en cuenta que en Internet se encuentran conectadas redes de tamaños muy diversos, se establecieron tres clases diferentes de direcciones, las cuales se representan mediante tres rangos de valores:

- Clase A: Son las que en su primer byte tienen un valor comprendido entre 1 y 126, incluyendo ambos valores. Estas direcciones utilizan únicamente este primer byte para identificar la red, quedando los otros tres bytes disponibles para cada uno de los computadores que pertenezcan a esta misma red. Esto significa que podrán existir más de dieciséis millones de ordenadores en cada una de las redes de esta clase. Este tipo de direcciones es usado por redes muy extensas, pero hay que tener en cuenta que sólo puede haber 126 redes de este tamaño.

- Clase B: Estas direcciones utilizan en su primer byte un valor comprendido entre 128 y 191, incluyendo ambos valores. En este caso el identificador de la red se obtiene de los dos primeros bytes de la dirección, teniendo que ser un valor entre 128.1 y 191.254 (no es posible utilizar los valores 0 y 255 por tener un significado especial). Los dos últimos bytes de la dirección constituyen el identificador del host permitiendo, por consiguiente, un número máximo de 64516 ordenadores en la misma red.

- Clase C: En este caso el valor del primer byte tendrá que estar comprendido entre 192 y 223, incluyendo ambos valores. Este tercer tipo de direcciones utiliza los tres primeros bytes para el número de la red, con un rango desde 192.1.1 hasta 223.254.254. De esta manera queda libre un byte para el computador, lo que permite que se conecten un máximo de 254 computadores en cada red. Estas direcciones permiten un menor número de computadores que las anteriores, aunque son las más numerosas pudiendo existir un gran número redes de este tipo (más de dos millones).

- Clase D: Las direcciones de esta clase están reservadas para multicasting que son usadas por direcciones de computadores en áreas limitadas.

- Clase E: Son direcciones que se encuentran reservadas para su uso futuro.

**Tabla de direcciones IP de Internet.**

| Clase | Primer byte | Identificación de red | Identificación de hosts | Número de redes | Número de hosts |
|---|---|---|---|---|---|
| A | 1 … 126 | 1 byte | 3 byte | 126 | 16.387.064 |
| B | 128 … 191 | 2 byte | 2 byte | 16.256 | 64.516 |
| C | 192 … 223 | 3 byte | 1 byte | 2.064.512 | 254 |

En la clasificación de direcciones anterior se puede notar que ciertos números no se usan. Algunos de ellos se encuentran reservados para un posible uso futuro, como es el caso de las direcciones cuyo primer byte sea superior a 223 (clases D y E, que aún no están definidas), mientras que el valor 127 en el primer byte se utiliza en algunos sistemas para propósitos especiales.

También es importante notar que los valores 0 y 255 en cualquier byte de la dirección no pueden usarse normalmente por tener otros propósitos específicos.
El número 0 está reservado para las máquinas que no conocen su dirección, pudiendo utilizarse tanto en la identificación de red para máquinas que aún no conocen el número de red a la que se encuentran conectadas, en la identificación de computador para máquinas que aún no conocen su número dentro de la red, o en ambos casos.

El número 255 tiene también un significado especial, puesto que se reserva para el broadcast. El broadcast es necesario cuando se pretende hacer que un mensaje sea visible para todos los sistemas conectados a la misma red. Esto puede ser útil si se necesita enviar el mismo datagrama a un número determinado de sistemas, resultando más eficiente que enviar la misma información solicitada de manera individual a cada uno. Otra situación para el uso de broadcast es cuando se quiere convertir el nombre por dominio de un ordenador a su correspondiente número IP y no se conoce la dirección del servidor de nombres de dominio más cercano.

Lo usual es que cuando se quiere hacer uso del broadcast se utilice una dirección compuesta por el identificador normal de la red y por el número 255 (todo unos en binario) en cada byte que identifique al computador. Sin embargo, por conveniencia también se permite el uso del número 255.255.255.255 con la misma finalidad, de forma que resulte más simple referirse a todos los sistemas de la red.
El broadcast es una característica que se encuentra implementada de formas diferentes dependiendo del medio utilizado, y por lo tanto, no siempre se encuentra disponible.

**ISATAP (INTRA-SITE AUTOMATIC TUNNELING ADDRESSING PROTOCOL)**
Protocolo de direccionamiento de túneles internos automáticos. Una tecnología de coexistencia que proporciona conectividad IPv6 unicast entre máquinas IPv6 situadas en una intranet IPv4. ISATAP, obtiene un identificador de interfaz a partir de la dirección IPv4 (pública o privada) asignada a la máquina. Este identificador se utiliza para el establecimiento de túneles automáticos a través de la infraestructura IPv4.

**LAN**
Abreviatura de Local Área Network (Red de Área Local o simplemente Red Local). Una red local es la interconexión de varios ordenadores y periféricos. Su extensión esta limitada físicamente a un edificio o a un entorno de unos pocos kilómetros. Su aplicación más extendida es la interconexión de ordenadores personales y estaciones de trabajo en oficinas, fábricas, entre otros; para compartir recursos e intercambiar datos y aplicaciones. En definitiva, permite que dos o más máquinas se comuniquen. El término red local incluye tanto el hardware como el software necesario para la interconexión de los distintos dispositivos y el tratamiento de la información.

**MODELO ISO/OSI**
Este modelo se basa en la definición de la arquitectura de la red (o sea la disposición de cada función requerida en la red) como un conjunto de capas o niveles funcionales. Cada nivel realiza unas funciones definidas que constituyen un servicio que se presenta al nivel inmediatamente superior. Cada nivel se comunica solamente con los niveles adyacentes a través de una interfaz. Al nivel

superior se le prestan servicios, al inferior se le solicitan servicios. Cuando dos nodos en la red están en comunicación, cada uno dispone de una implementación del modelo OSI.
El modelo OSI consta de 7 capas o Niveles consecutivos, denominados del nivel más bajo al más alto así:

Nivel Físico, de Enlace, de Transporte, de Sesión, de Presentación y de Aplicación.

**MTU**
Unidad máxima de transferencia (Maximum Transfer Unit - MTU) es un término informático que expresa el tamaño en bytes del datagrama más grande que puede pasar por una capa de un protocolo de comunicaciones.

Es la unidad de datos del protocolo más grande que se puede enviar. Las unidades máximas de transmisión se definen a nivel de enlace (tamaño máximo de trama) y a nivel de red o de Internet (tamaño máximo de los paquetes IPv6).

**MTU DE LA RUTA**
Tamaño máximo de un paquete IPv6 que puede enviarse sin emplear fragmentación entre una fuente y un destino sobre una ruta en una red IPv6. La MTU de la ruta coincide con la menor MTU de enlace para todos los enlaces de dicha ruta.

**MTU DEL ENLACE**
La unidad de transmisión máxima (MTU) -número de bytes en el paquete IPv6 más grande- que puede enviarse sobre el enlace. Dado que el tamaño máximo de trama incluye las cabeceras y colas de nivel de enlace, la MTU del enlace no coincide con el tamaño máximo de trama del enlace. La MTU del enlace coincide con el máximo tamaño de carga útil de la tecnología de nivel de enlace.

**MTU IPv6**
El tamaño máximo de un paquete IP que se puede enviar sobre un enlace.

**NODO**
Espacio real en el que confluyen parte de las conexiones de otros espacios reales o abstractos que comparten sus mismas características y que a su vez también son nodos. Todos estos nodos se interrelacionan entre sí de una manera no jerárquica y conforman lo que en términos sociológicos o matemáticos le llamamos red.

**NODO CORRESPONSAL**
Un nodo que se comunica con un nodo móvil que se encuentra fuera de su red propia.

**NODO IPv4**
Un nodo que implementa IPv4; puede enviar y recibir paquetes IPv4. Puede ser un nodo con soporte sólo IPv4 o un nodo dual IPv4/IPv6.

**NODO IPv6**
Nodo que implementa IPv6; puede enviar y recibir paquetes IPv6. Un nodo IPv6 puede ser bien un nodo con soporte IPv6 o un nodo dual IPv6/IPv4.

**NODO IPv6/IPv4**
Es un nodo que dispone de implementaciones de IPv4 e IPv6.

**NOTACIÓN HEXADECIMAL SEPARADA CON DOS PUNTOS (COLON HEXADECIMAL NOTATION)**
La notación empleada para expresar direcciones IPv6. La dirección de 128 bits es dividida en 8 bloques de 16 bits. Cada bloque se expresa como un número hexadecimal y éstos se separan del siguiente por medio del signo ortográfico dos puntos (:). Dentro de cada bloque, los ceros situados a la izquierda son eliminados. Un ejemplo de una dirección IPv6 unicast representada en notación hexadecimal separada por dos puntos es 3FFE:FFFF:2A1D:48C:2AA:3CFF:FE21:81F9.

**NOTACIÓN PREFIJO-LONGITUD**
Notación mediante la cual se expresan los prefijos de red. Tiene la forma dirección/longitud del prefijo, siendo dicha longitud el número de bits iniciales de la dirección que se fijan para definir el prefijo.

**PAQUETE**
Unidad fundamental de transporte de información en todas las redes de computadoras modernas. El término datagrama es usado a veces como sinónimo.
Un paquete está generalmente compuesto de tres elementos: una cabecera (header en inglés) que contiene generalmente la información necesaria para trasladar el paquete desde el emisor hasta el receptor, el área de datos (payload en inglés) que contiene los datos que se desean trasladar, y la cola (trailer en inglés), que comúnmente incluye código de detección de errores.

**PDU**
Unidad de datos del protocolo. Conjunto de datos correspondiente a una capa concreta en una arquitectura de red en capas. La unidad de datos de la unidad n se convierte en la carga útil de la capa n-1 (la capa inferior).

**PREFIJO DE FORMATO**
Los bits de orden alto con un valor fijo que definen un tipo de dirección IPv6.

**PREFIJO DE RED**
Es la parte fija de la dirección que se utiliza para determinar el identificador de la subred, la ruta o el rango de direcciones.

**PREFIJO DE SITIO**
Típicamente un prefijo de 48 bits que se utiliza para referirse a todas las direcciones del sitio. Los prefijos de sitio se almacenan en una tabla de prefijos que se emplea para confinar todo el tráfico asociado a esos prefijos dentro del sitio.

**PROTOCOLO DE INTERNET**
Soporte lógico básico empleado para controlar sistemas de redes. Este protocolo especifica cómo las computadoras de puerta encaminan la información desde el ordenador emisor hasta el ordenador receptor. Otro protocolo denominado Protocolo de Control de Transmisión (TCP) comprueba si la información ha llegado al ordenador de destino y, en caso contrario, hace que se vuelva a enviar. La utilización de protocolos TCP/IP es un elemento común en las redes Internet e intranet.

**PROTOCOLO DEL NIVEL SUPERIOR**
Protocolo que utiliza IPv6 como transporte y se sitúa en la capa inmediatamente superior a IPv6, como ICMPv6, TCP y UDP.

**PROTOCOLO PUNTO-A-PUNTO**
Método de encapsulación de red punto-a-punto que proporciona delimitadores de tramas, identificación del protocolo y servicios de integridad a nivel de bit.

**PSEUDO-CABECERA**
Cabecera temporal que se construye para calcular el checksum necesario para asociar la cabecera IPv6 con la carga. En IPv6 se utiliza un nuevo formato de pseudo-cabecera al calcular el checksum de UPD, TCP y ICMPv6.

**RED**
Dos o más subredes conectadas por routers. Otro término empleado es interred.

**REDIRECCIONAR**
Procedimiento englobado dentro de los mecanismos de descubrimiento de vecinos por el cual se informa a un host de la dirección IPv6 de otro que resulta más adecuado como siguiente salto hacia un determinado destino.

**REENSAMBLADO**
Proceso mediante el cual se reconstruye la carga original de un datagrama a partir de varios fragmentos.

**RESOLUCIÓN DE DIRECCIONES**
Proceso de resolución de direcciones del nivel de enlace para la dirección de next-hop (siguiente salto, gateway) en un enlace.

**RESOLUCIÓN DE NOMBRES**
Es el proceso de obtención de una dirección a partir de un nombre. En IPv6, la resolución de nombres permite obtener direcciones a partir de nombres de equipos o nombres de dominio totalmente cualificado (FQDN).

**RFC**
Acrónimo inglés de Request For Comments. Conjunto de notas técnicas y organizativas donde se describen los estándares o recomendaciones de Internet (originalmente ARPANET), comenzado en 1969.
En el caso de la informática, están hechos para hacer compatibles los programas entre sí y que se pueda usar diferente software para la misma función. Definen protocolos y lenguajes, se garantiza la interoperabilidad entre sistemas si ambos cumplen el mismo RFC.

**ROUTER**
Dispositivo de hardware y software de interconexión de redes de ordenadores/computadoras que opera en la capa tres (nivel de red) del modelo OSI. Este dispositivo interconecta segmentos de red o redes enteras. Hace pasar paquetes de datos entre redes tomando como base la información de la capa de red.

El router toma decisiones lógicas con respecto a la mejor ruta para el envío de datos a través de una red interconectada y luego dirige los paquetes hacia el segmento y el puerto de salida adecuados.

**ROUTER 6TO4**
Router para favorecer la coexistencia con IPv4, que proporciona conectividad unicast entre redes y máquinas IPv6 a través de una infraestructura IPv4. 6to4 utiliza una dirección pública IPv4 para construir un prefijo global IPv6.

**ROUTER ISATAP**
Un router IPv6/IPv4 que responde a las solicitudes de equipos ISATAP a través de túneles y encamina el tráfico entre equipos y nodos ISATAP de otra red o subred ISATAP.

**RUTA ASOCIADA A UNA SUBRED**
Ruta cuyo prefijo de 64 bits corresponde al de una subred en concreto.

**RUTA POR DEFECTO**
La ruta con prefijo ::/0. La ruta de defecto, recoge todos los destinos y es la ruta empleada para obtener la siguiente dirección de destino cuando no hay otras rutas coincidentes.

**SUBRED**
Cuando una red de computadoras se vuelve muy grande, conviene dividirla en subredes, por los siguientes motivos:

- Reducir el tamaño de los dominios de broadcast.

- Hacer la red más manejable, administrativamente. Entre otros, se puede controlar el tráfico entre diferentes subredes, mediante ACLs.

Para conectar diferentes subredes entre sí, se requiere un router u otro equipo similar (uno que opera en la capa 3 del modelo OSI).

En el caso más simple, se puede dividir una red en subredes de tamaño fijo (todas las subredes tienen el mismo tamaño). Sin embargo, por la escasez de direcciones IP, hoy en día frecuentemente se usan subredes de tamaño variable.

**SWITCH**
Dispositivo de interconexión de redes de ordenadores/computadoras que opera en la capa 2 (nivel de enlace de datos) del modelo OSI (Open Systems Interconection). Un switch interconecta dos o más segmentos de red, pasando datos de una red a otra, de acuerdo con la dirección MAC de destino de los datagramas en la red.

Los switches se utilizan cuando se desea conectar múltiples redes y ordenadores. Al igual que los bridges, dado que funcionan como un filtro en la red, mejoran el rendimiento y la seguridad de las LANs (Local Area Network- Red de Área Local).

**TCP**
Protocolo de Control de Transmisión. Es uno de los protocolos fundamentales en Internet. Muchos programas dentro de una red de datos compuesta por ordenadores pueden usar TCP para crear conexiones entre ellos a través de las cuales enviarse datos. El protocolo garantiza que los datos serán entregados en su destino sin errores y en el mismo orden en que se transmitieron. También

proporciona un mecanismo para distinguir distintas aplicaciones dentro de una misma máquina, a través del concepto de puerto.

**TRAMA**
Es una unidad de envío de datos. Viene a ser sinónimo de paquete de datos o Paquete de red, aunque se aplica principalmente en los niveles OSI más bajos, especialmente en el nivel de enlace de datos.

Normalmente una trama constará de cabecera, datos y cola. En la cola suele estar algún chequeo de errores. En la cabecera habrá campos de control de protocolo. La parte de datos es la que quiera transmitir en nivel de comunicación superior, típicamente el Nivel de red.

**TÚNEL**
Un túnel IPv6 sobre IPv4, en los que los puntos finales son determinados por configuración manual.

**TÚNEL AUTOMÁTICO**
Un túnel IPv6 sobre IPv4 en el que los puntos finales son determinados por el empleo de interfaces lógicos de túneles, rutas y direcciones orígenes y destino IPv6.

**TÚNEL MÁQUINA-A-MÁQUINA**
Un tunelado IPv6 sobre IPv4 en el que los dos extremos son máquinas.

**TÚNEL MÁQUINA-A-ROUTER**
Un tunelado IPv6 sobre IPv4 en el que el túnel empieza en un host y acaba en un router IPv6/IPv4.

**TÚNELES IPv6 AUTOMÁTICOS**
Creación automática de túneles que se emplea con direcciones compatibles con IPv4.

**TÚNELES IPv6 SOBRE IPv4**
Consiste en enviar paquetes IPv6 con una cabecera IPv4, de forma que el tráfico IPv6 pueda enviarse sobre una infraestructura IPv4. En la cabecera IPv4, el campo de Protocolo toma el valor 41.

**VECTOR DE DISTANCIA**
Una tecnología para protocolos de rutado que propaga información de rutado en la forma de un identificador de red y su distancia en número de saltos.

**VECTOR DE RUTA**

Se trata de una tecnología de protocolo de rutado que intercambia secuencias de información de saltos indicando el camino a seguir en una ruta. Por ejemplo, BGP-4 intercambia secuencias de números de sistemas autónomos. Un sistema autónomo es una porción de la red perteneciente a la misma autoridad administrativa.

## LISTA DE TABLAS

## CONTENIDO

# CAPITULO I

# CAPITULO I: GENERALIDADES DE LA ARQUITECTURA ACTUAL.

## 1.1. HISTORIA DE INTERNET

La red Internet surgió de un programa de investigación realizado por la Defense Advanced Research Projects Agency (CARPA) de Estados Unidos, que se centró en formas de enlazar varias redes informáticas. El resultado de este programa fue ARPANET, que empezó a funcionar en 1969. En 1971 había aproximadamente 40 computadoras, o sistemas, conectados a ARPANET y los investigadores estaban desarrollando la capacidad de enviar correo electrónico entre redes. ARPANET continuó creciendo durante los años 70 y empezaron a conectarse también otras redes informáticas.

La investigación sobre las comunicaciones entre redes llevó al desarrollo de los protocolos de red TCP/IP, que sustituyeron al anterior conjunto de protocolos llamado NCP, y que se convirtió en el estándar de ARPANET. Según fueron sumándose más redes a ARPANET, este inmenso entramado de redes pasó a ser conocido como Internet. La red original ARPANET se clausuró en 1990, pasando el relevo a Internet.

Internet ha experimentado un ritmo de crecimiento asombroso en los últimos diez años. En 1984 había aproximadamente 1,000 servidores en Internet. En 1989, este número había crecido a más de 100,000 y, tres años después, en 1992, se contabilizaban un total de más de un millón de computadoras conectada a Internet. En julio de 1994 había más de 3 millones de sistemas informáticos conectados a la red, con unos 20 millones de usuarios. Con el desarrollo de herramientas de recuperación de información de fácil manejo, como Mosaic y la World Wide Web, muchos usuarios normales empezaron a descubrir los muchos recursos accesibles de información que incorpora Internet.

En cuanto al tamaño geográfico de Internet, la red en realidad cubre el mundo entero. Casi todos los países industrializados tienen algún tipo de conectividad a Internet.

Con tantos millones de usuario en Internet, ¿Cómo especificar el usuario con el que se desea comunicarse?, para ello es necesario conocer el nombre de la computadora, así como necesita conocer el nombre y dirección de alguien cuando se le desea enviar una carta. Estos nombres vienen determinados por una convención llamada Sistema de Nombres de Dominio (DNS) y se encuentran detallados en las Peticiones de Comentarios (RFC) de Internet, rfc1032, rfc1033, rfc1034 y rfc1035.

## 1.2. MODELO OSI.

Durante las últimas dos décadas ha habido un enorme crecimiento en la cantidad y tamaño de las redes. Muchas de ellas sin embargo, se desarrollaron utilizando implementaciones de hardware y software diferentes. Como resultado, muchas de las redes eran incompatibles y se volvió muy difícil para las redes que utilizaban especificaciones distintas poder comunicarse entre sí. Para solucionar este problema, la Organización Internacional para la Normalización (ISO) realizó varias investigaciones acerca de los esquemas de red. La ISO reconoció que era necesario crear un modelo de red que pudiera ayudar a los diseñadores de red a implementar redes que pudieran comunicarse y trabajar en conjunto (interoperabilidad) y por lo tanto, elaboraron el modelo de referencia OSI en 1984.

Para que los paquetes de datos puedan viajar desde el origen hasta su destino a través de una red, es importante que todos los dispositivos de la red hablen el mismo lenguaje o protocolo. Un protocolo es un conjunto de reglas que hacen que la comunicación en una red sea más eficiente.

Una definición técnica de un protocolo de comunicaciones de datos es: un conjunto de normas, o un acuerdo, que determina el formato y la transmisión de datos. La capa n de un computador se comunica con la capa n de otro computador. Las normas y convenciones que se utilizan en esta comunicación se denominan colectivamente protocolo de la capa n.

Al principio de su desarrollo, las LAN, MAN y WAN eran en cierto modo caótico. A principios de la década de los 80 se produjeron tremendos aumentos en la cantidad y el tamaño de las redes. A medida que las empresas se dieron cuenta de que podrían ahorrar mucho dinero y aumentar la productividad con la tecnología de networking, comenzaron a agregar redes y a expandir las redes existentes casi simultáneamente con la aparición de nuevas tecnologías y productos de red.

A mediados de los 80, estas empresas debieron enfrentar problemas cada vez más serios debido a su expansión caótica. Resultaba cada vez más difícil que las redes que usaban diferentes especificaciones pudieran comunicarse entre sí. Se dieron cuenta que necesitaba salir de los sistemas de networking propietarios.

Los sistemas propietarios se desarrollan, pertenecen y son controlados por organizaciones privadas. En la industria informática, propietario es lo opuesto de abierto, y significa que una empresa o un pequeño grupo de empresas controlan el uso de la tecnología. Abierto significa que el uso libre de la tecnología está disponible para todos.

Para enfrentar el problema de incompatibilidad de las redes y su imposibilidad de comunicarse entre sí, la Organización Internacional para la Normalización (ISO) estudió esquemas de red como DECNET, SNA y TCP/IP a fin de encontrar un conjunto de reglas. Como resultado de esta investigación, la ISO desarrolló un modelo de red que ayudaría a los fabricantes a crear redes que fueran compatibles y que pudieran operar con otras redes.

El proceso de dividir comunicaciones complejas en tareas más pequeñas y separadas se podría comparar con el proceso de construcción de un automóvil. Visto globalmente, el diseño, la fabricación y el ensamblaje de un automóvil es un proceso de gran complejidad. Es poco probable que una sola persona sepa cómo realizar todas las tareas requeridas para la construcción de un automóvil desde cero. Es por ello que los ingenieros mecánicos diseñan el automóvil, los ingenieros de fabricación diseñan los moldes para fabricar las partes y los técnicos de ensamblaje ensamblan una parte del auto.

El modelo de referencia OSI (Nota: No debe confundirse con ISO.), Lanzado en 1984, fue el esquema descriptivo que crearon. Este modelo proporcionó a los fabricantes un conjunto de estándares que aseguraron una mayor compatibilidad e interoperabilidad entre los distintos tipos de tecnología de red utilizados por las empresas a escala mundial.

El modelo de referencia OSI es el modelo principal para las comunicaciones por red. Aunque existen otros modelos, en la actualidad la mayoría de los fabricantes de redes relacionan sus productos con el modelo de referencia OSI, especialmente cuando desean enseñar a los usuarios cómo utilizar sus productos.

El modelo de referencia OSI permite que los usuarios vean las funciones de red que se producen en cada capa. Más importante aún, el modelo de referencia OSI es un marco que se puede utilizar para comprender cómo viaja la información a través de una red. Además, puede usar el modelo de referencia OSI para visualizar cómo la información o los paquetes de datos viajan desde los programas de aplicación (por Ej., Hojas de cálculo, documentos, etc.), a través de un entorno de red (por Ej., Cables, etc.), hasta otro programa de aplicación ubicado en otro computador de la red, aún cuando el remitente y el receptor tengan distintos tipos de red.

En el modelo de referencia OSI, hay siete capas numeradas, cada una de las cuales ilustra una función de red particular. Esta división de las funciones de networking se denomina división en capas.

El problema de trasladar información entre computadores se divide en siete problemas más pequeños y de tratamiento más simple en el modelo de referencia

OSI. Cada uno de los siete problemas más pequeños está representado por su propia capa en el modelo. Las siete capas del modelo de referencia OSI se muestran en la figura 1-1:


**Fig. 1-1. Modelo OSI**

Cada capa individual del modelo OSI tiene un conjunto de funciones que debe realizar para que los paquetes de datos puedan viajar en la red desde el origen hasta el destino. A continuación, presentamos una breve descripción de cada capa del modelo de referencia OSI tal como aparece en la figura 1-1.

**Capa 7: La capa de aplicación**

La capa de aplicación es la capa del modelo OSI más cercana al usuario; suministra servicios de red a las aplicaciones del usuario. Difiere de las demás capas debido a que no proporciona servicios a ninguna otra capa OSI, sino solamente a aplicaciones que se encuentran fuera del modelo OSI. Algunos ejemplos de dichos procesos de aplicación son los programas de hojas de cálculo, de procesamiento de texto y los de las terminales bancarias.

**Capa 6: La capa de presentación**

La capa de presentación garantiza que la información que envía la capa de aplicación de un sistema pueda ser leída por la capa de aplicación de otro. De ser

necesario, la capa de presentación traduce entre varios formatos de datos utilizando un formato común.

**Capa 5: La capa de sesión**

Como su nombre lo implica, la capa de sesión establece, administra y finaliza las sesiones entre dos hosts que se están comunicando. La capa de sesión proporciona sus servicios a la capa de presentación. También sincroniza el diálogo entre las capas de presentación de los dos hosts y administra su intercambio de datos. Además de regular la sesión, la capa de sesión ofrece disposiciones para una eficiente transferencia de datos, clase de servicio y un registro de excepciones acerca de los problemas de la capa de sesión, presentación y aplicación.

**Capa 4: La capa de transporte**

La capa de transporte segmenta los datos originados en el host emisor y los reensambla en una corriente de datos dentro del sistema del host receptor. El límite entre la capa de sesión y la capa de transporte puede imaginarse como el límite entre los protocolos de capa de medios y los protocolos de capa de host.

Mientras que las capas de aplicación, presentación y sesión están relacionadas con aspectos de las aplicaciones, las tres capas inferiores se encargan del transporte de datos.

La capa de transporte intenta suministrar un servicio de transporte de datos que aísla las capas superiores de los detalles de implementación del transporte.

Específicamente, temas como la confiabilidad del transporte entre dos hosts es responsabilidad de la capa de transporte. Al proporcionar un servicio de comunicaciones, la capa de transporte establece, mantiene y termina adecuadamente los circuitos virtuales. Al proporcionar un servicio confiable, se utilizan dispositivos de detección y recuperación de errores de transporte.

**Capa 3: La capa de red**

La capa de red es una capa compleja que proporciona conectividad y selección de ruta entre dos sistemas de hosts que pueden estar ubicados en redes geográficamente distintas. Si se desea recordar la Capa 3, se debe pensar en selección de ruta, conmutación, direccionamiento y enrutamiento.

**Capa 2: La capa de enlace de datos**

La capa de enlace de datos proporciona un tránsito de datos confiable a través de un enlace físico. Al hacerlo, la capa de enlace de datos se ocupa del direccionamiento físico (comparado con el lógico), la topología de red, el acceso a la red, la notificación de errores, y entrega ordenada de tramas.

**Capa 1: La capa física**

La capa física define las especificaciones eléctricas, mecánicas, de procedimiento y funcionales para activar, mantener y desactivar el enlace físico entre sistemas finales. Las características tales como niveles de voltaje, temporización de cambios de voltaje, velocidad de datos físicos, distancias de transmisión máximas, conectores físicos y otros atributos similares se definen a través de las especificaciones de la capa física. Si se desea recordar la Capa 1, se debe pensar en señales y medios.

## 1.3. DEFINICIÓN DE TCP/IP.

Aunque el modelo de referencia OSI sea universalmente reconocido, el estándar abierto de Internet desde el punto de vista histórico y técnico es el Protocolo de control de Transmisión / Protocolo Internet (TCP/IP). El modelo de referencia TCP/IP y la pila de protocolo TCP/IP hacen que sea posible la comunicación entre dos computadores, desde cualquier parte del mundo, a casi la velocidad de la luz. El modelo TCP/IP tiene importancia histórica, al igual que las normas que permitieron el desarrollo de la industria telefónica, de energía eléctrica, el ferrocarril, la televisión y las industrias de vídeos.

El TCP/IP es una colección de protocolos estándar de la industria diseñada para intercomunicar grandes redes.

A continuación se presentan algunos conceptos sobre TCP/IP, su terminología y explicación de como la Internet Society crea el estándar de Internet.

### 1.3.1. Historia del TCP/IP

El TCP/IP fue originado con los experimentos de intercambio de paquetes dirigido por el U.S. Department of Defense Advanced Research Projects Agency (DARPA) durante la década de 1960 a 1970.

Hay varios hitos importantes en la historia del TCP/IP:

**1970:** Los ordenadores de la Advanced Research Agency Network (ARPANET) comienzan a utilizar el NCP (Network Control Protocolo).

**1972:** La primera especificación Telnet. “ad hoc telnet protocol” se define como una RFC, la 318.

**1973:** RFC 454. Se introduce el FTP (File Transport Protocol).

**1974:** El TCP (Transmisión Control Protocol) se especifica detalladamente.

**1981:** El estándar IP se publica en la RFC 791.

**1982:** La ‘Defense Communications Agency’ (DCA) y ARPA establecen a la ‘Transmision Control Protocol (TCP) y al Internet Protocol (IP)” como la colección de protocolos TCP/IP.

**1983:** ARPANET cambia de NCP a TCP/IP.

**1984:** Se define el concepto de DNS (Domain Name System).

### 1.3.2. El proceso de estandarización de Internet.

Surge un grupo internacional de voluntarios llamado Internet Society para administrar la colección de protocolos TCP/IP. Los estándares para el TCP/IP son publicados en una serie de documentos llamados Request For Comments, o simplemente RFCs. Debemos tener presente que Internet nació como libre y sigue como libre. Por tanto esta no es una organización “propietaria” de Internet o de sus tecnologías. Únicamente son responsables de su dirección.

**ISOC:** Internet Society, fue creada en 1992 como una organización global responsable de las tecnologías de trabajo en Internet y las aplicaciones de Internet. Su principal propósito es animar al desarrollo y la disponibilidad de Internet.

**IAB:** Internet Architecture Board, es el grupo técnico de la ISOC responsable de las opciones estándar de Internet, publicar las RFCs y vigilar los procesos estándar de Internet.

El IAF dirige la IETF (Internet Engineering Task Force), IANA (Internet Assigned Numbers Authority) y la IRTF (Internet Research Task Force). La IETF desarrolla los estándares y protocolos Internet, y vigila y desarrolla soluciones a problemas técnicos alrededor de Internet. La IANA vigila y coordina la asignación

de un identificador único en Internet: Las direcciones IP. El grupo IRTF es el responsable de la coordinación de todos los proyectos relacionados con el TCP/IP.

**RFCs:** Request for Comments, Los RFCs describen todo el trabajo interno en Internet. El estándar TCP/IP es siempre publicado como una RFC, pero no todas las RFCs especifican estándares.

El TCP/IP estándar, no ha sido desarrollado por un comité. Ha sido desarrollado "por consenso". Cualquier miembro de la Internet Society puede publicar un documento como una SFC. El documento es revisado por un grupo de expertos y se le asigna una clasificación. Hay cinco géneros de clasificaciones en las RFCs:

**Required (Requerido):** Debe ser implementado en todas las maquinas que ejecuten TCP/IP inclusive los Gateway y routers.

**Recommended (Recomendada):** Se estimula el que todas las maquinas que ejecuten TCP/IP utilicen esta especificación de la RFC. Las RFC recomendadas, normalmente están siendo utilizadas en todas las maquinas.

**Elective:** El uso de esta RFC es opcional. No es ampliamente usada.

**Limited Use (Uso Limitado):** No esta pensada para un uso general.

**Not Recommended (No Recomendada):** No está aconsejada su uso.

Si un documento comienza a ser considerado como un estándar, comienza a pasar por los diferentes estados de desarrollo, prueba y aceptación. Durante este proceso, estos procesos son formalmente llamados `Maturity Levels` (Niveles de Maduración). Hay tres niveles de maduración en los estándares de Internet:

- ✓ **Proposed Standard (Propuesta):** Una especificación de propuesta, es generalmente estable, ha resuelto las conocidas alternativas de diseño, está bien comprendida, ha recibido el visto bueno de la comunidad y parece un buen candidato a ser evaluado por la comunidad.

- ✓ **Draft Standard (Borrador):** Un borrador, debe ser entendido y reconocido como estable, tanto semánticamente como su base para poder ser desarrollada correctamente.

- ✓ **Internet Standard:** El estándar Internet, (muchas veces nos referimos a él como un "estándar" simplemente) se caracteriza por un alto grado de madurez técnica y generalmente se reconoce como una ayuda al protocolo o al servicio que significa un beneficio para la comunidad Internet.

Cuando se publica un documento, se le asigna un número de RFC. Este número original, nunca va a cambiar. Si esta RFC requiera cambios, se publica una nueva RFC con un nuevo numero.
La IAB publica el "IAB Oficial Protocol Standard" trimestralmente.

### 1.3.3. El modelo de capa de TCP/IP

**Capa de Red:** Las base de este modelo de capas de interface de red. Esta capa es la responsable de enviar y recibir tramas, las cuales son los paquetes de información que viajan en una red como una 'unidad simple'. La capa de red, envía tramas a la red, y recupera tramas de la red.

**Capa de Internet:** Esta capa encapsula paquetes en datagramas Internet y además esta capa ejecuta todos los algoritmos de enrutamiento (routing) de paquetes. Los cuatros protocolos Internet son: Internet Protocol (IP), Address Resolution Protocol (ARP), Internet Control Message Protocol (ICMP) y Internet Group Management Protocol (IGMP).

- **IP:** Es el responsable del envío y enrutamiento de paquetes entre maquinas y redes.

- **ARP:** Obtiene las direcciones de hardware de las maquinas situadas en la misma red física. Recordemos que la dirección física de cada tarjeta de red es única en el mundo. Dicha dirección "física" ha sido implementada vía hardware por el fabricante de la tarjeta de red, y dicho fabricante, lo selecciona de un rango de direcciones único asignado a él y garantiza la unicidad de dicha tarjeta. Este caso es el más corriente y es el de las tarjetas de red Ethernet. Existe para otras topologías de red, igualmente una asignación única hardware de reconocimiento de la tarjeta.

- **ICMP:** Envía mensajes e informa de errores en el envío de paquetes.

- **IGMP:** Se utiliza para la comunicación entre routers (Enrutadores de Internet).

**Capa de Transporte:** La capa de transporte, nos da el nivel de "sesión" en la comunicación. Los dos protocolos posibles de transporte son TCP (Transmisión Control Protocol) y UDP (User Datagram Protocol). Se puede utilizar uno u otro protocolo dependiendo del método preferido de envío de datos.

El TCP nos da un tipo de conectividad “orientado a conexión”. Típicamente se utiliza para transferencia de largas cantidades de datos de una sola vez. Se utiliza también en aplicaciones que requieren un “reconocimiento” o validación (ACK: acknowledgment) de los datos recibidos.

El UDP proporciona conexión de comunicación y no garantiza la entrega de paquetes. Las aplicaciones que utilicen UDP normalmente envían pequeñas cantidades de datos de una sola vez. La aplicación que lo utilice, es la responsable en este caso de la integridad de los paquetes y debe establecer sus propios mecanismos para pedir repetición de mensaje, seguimiento, etc. No existiendo ni garantía de entrega ni garantía del orden de entrega en la maquina destino.

**Capa de Aplicación:** En la cima de este modelo, está la capa de aplicación.
Esta es la capa que las aplicaciones utilizan para acceder a la red. Existen muchas utilidades y servicios en la capa de aplicación, por ejemplo: FTP, Telnet, SNMP y DNS.

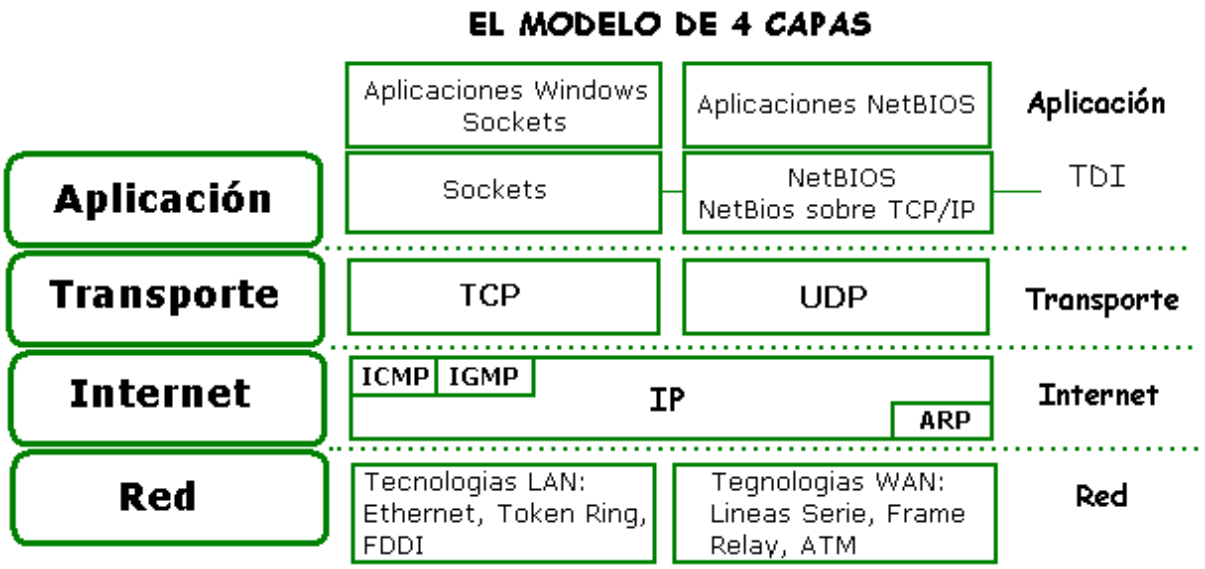



**Fig. 1-2. Modelo TCP/IP de 4 Capas.**

### 1.3.4. TCP.

TCP es un servicio de entrega orientado a la conexión. Es totalmente fiable.

Los datos TCP se transmiten en segmentos y se establece una sesión antes de que las maquinas puedan intercambiar datos. TCP usa comunicaciones en flujo de bytes, es decir, los datos son considerados una secuencia de bytes.

Se consigue la seguridad asignando un número de secuencia a cada segmento transmitido por el TCP. La recepción de un ACK nos confirma la llegada correcta de un segmento a la otra maquina. Por cada segmento enviado, el receptor debe devolver un ACK en un periodo de tiempo especificado.

Si el emisor no recibe un ACK, entonces el dato se vuelve a transmitir. Si el segmento se recibe dañado el receptor lo descarta inmediatamente. Debido a que el ACK no se envía en este caso, el emisor retransmitirá el segmento.

**PUERTOS TCP.**

Las aplicaciones 'sockets' se identifican a si mismas de manera única en una maquina por usar un 'protocol port number'. Por ejemplo, un servidor FTP usa un determinado puerto TCP para que otras aplicaciones puedan comunicarse con él.

Los puertos pueden usar cualquier número entre 0 y 65536. Los números de puerto de cara a aplicaciones "cliente" son dinámicamente asignados por el sistema operativo cuando se solicita una petición para este servicio. Los números de puertos de las aplicaciones servidoras web-known (bien conocidos) han sido preasignados por el IANA (Internet Assigned Numbers Authority) y no pueden cambiarse.

Los puertos web-known están en el rango del 1 al 1024. La lista completa está documentada en la RFC 1700.

Un puerto TCP nos da una localización para la entrega de mensajes. Los números de puerto inferiores a 256 son definidos como los puertos mas corrientemente usados. Por ejemplo podemos fijarnos en los siguientes puertos:

| | |
|---|---|
| **21** | FTP |
| **23** | TELNET |
| **53** | Domain Name System (DNS) |
| **139** | Servicio de Sesión NetBIOS |

**Tabla 1-1. Puertos TCP.**

## SESIONES TCP.

Una sesión TCP se inicia en tres vías. El propósito de estas tres vías es sincronizar el envío y la recepción de segmentos, informar a la otra maquina de la cantidad de datos que es capaz de recibir de una tachada y establecer una conexión virtual.

Estos son los pasos seguidos:

1. La maquina que inicia una sesión envía un segmento con el flag (bandera) de sincronización (SYN) activado.

2. La maquina receptora envía un ACK a la petición devolviendo un segmento con:

    - El flag de sincronización colocado.

    - Un número de secuencia que indica el byte de comienzo para el segmento que acaba de ser enviado.

    - Un ACK con el número de secuencia del primer byte del siguiente segmento que espera recibir.

3. El host peticionario vuelve a enviar un segmento con el número de secuencia ACK. En este momento la conexión queda establecida.

TCP utiliza un proceso similar para finalizar una conexión. Esto garantiza que ambas máquinas han terminado de transmitir y recibir todos los datos.

Los búferes TCP para transmisión entre dos máquinas se realizan utilizando ventanas. Cada máquina TCP mantiene dos ventanas: una para recibir y otra para enviar datos. El tamaño de las ventanas, indica la cantidad de datos que pueden mantenerse en los búferes en una de las máquinas.

## ESTRUCTURA DE LOS PAQUETES TCP.

Todos los segmentos TCP tienen dos partes: datos y cabecera. La tabla 1-2 lista los campos de la cabecera:

| CAMPO | FUNCIÓN |
|---|---|
| **Puerto Origen** | Puerto TCP de la máquina 'emisora' de datos. |
| **Puerto Destino** | Puerto TCP de la máquina destino. |
| **Numero de ACK** | El número de secuencia del próximo byte que se espera recibir. |
| **Longitud de datos** | Longitud del segmento TCP. |
| **Reservado** | Reservado para uso futuro. |
| **Flags** | Este campo especifica cual es el contenido del segmento. |
| **Ventana** | Cuanto espacio queda disponible en la ventana TCP. |
| **Checksum** | Número de control para verificar que la cabecera es correcta. |
| **Apuntador 'Urgente'** | Cuando se están enviando datos 'urgentes' (especificados así en el campo Flags) este campo apunta al final de los datos urgentes en el segmento. |

**Tabla 1-2. Estructura de los paquetes TCP.**

### 1.3.5 UDP.

"User Datagram Protocol" UDP es un servicio de envío de datagramas sin garantía de entrega. A este método se le denomina 'no orientado a la conexión' al contrario que el TCP que al establecer una sesión, se le denomina 'orientado a la conexión''. Por tanto, la llegada al destino de un datagrama o la secuencia correcta de entrega no está garantizada.

UDP se utiliza en las aplicaciones que no requieren un ACK (acknowledgement) de acuse de recibo de recepción de datos. Las aplicaciones que lo utilizan son típicamente las aplicaciones que transmiten pequeñas cantidades de datos a la vez. Por ejemplo, aplicaciones que lo utilizan son, el servicio de nombre NetBIOS

y el SNMP (Un protocolo de control de redes. No confundirlo con el SMTP de correo electrónico).

**PUERTOS UDP.**

Para utilizar UDP, una aplicación debe dar una dirección IP y un número de puerto de la aplicación destino. Un puerto, funciona como una cola de mensajes multiplexados que puede recibir múltiples mensajes al tiempo. Es importante resaltar que los puertos relacionados en la tabla 1-3 son puertos UDP y son distintos de los puertos TCP aún cuando algunos de ellos pueden tener el mismo número.

| | | |
|---|---|---|
| **15** | NETSTAT | Estado de la Red. |
| **53** | DOMAIN | DNS (Domain Name System) |
| **69** | TFTP | Trivial File Transfer Protocol |
| **137** | NETBIOS-NS | Servicio de nombres NETBIOS |
| **138** | NETBIOS-DGM | Servicio de datagramas NETBIOS |
| **161** | SNMP | Monitor de Red SNMP |

**Tabla 1-3. Puertos UDP**

El UDP está definido en la RFC 768.

## 1.4. PROTOCOLO DE INTERNET (IP)

IP es el protocolo primario de conexión responsable del envío y enrutamiento de paquetes entre maquinas (hosts), no establece una sesión antes de intercambiar datos y no es fiable debido a que trabaja sin garantía de entrega. A lo largo del camino, un paquete puede perderse, cambiarse de secuencia, duplicarse, retrasarse, o incluso trocearse.

IP no requiere una comunicación ACK (acknowledgment) cuando se reciben los datos. El Emisor o el Receptor no son informados cuando un paquete se pierde o

se envía fuera de secuencia. El ACK de los paquetes es responsabilidad de una capa de más alto nivel de transporte como por ejemplo el TCP.

Si el IP identifica una dirección de destino como una dirección 'local', el IP envía el paquete directamente a la maquina. Si el destino es identificado como un destino 'remoto', el IP chequea sus tablas de rutas. Si encuentra una ruta, el IP envía el paquete utilizando esa ruta. Si no encuentra una ruta, el IP envía el paquete al gateway por defecto (también llamado router o enrutador).

### 1.4.1. Estructura Del Paquete IP.

Los campos del paquete IP en la versión 4 del TCP/IP (versión actual) son los siguientes:

| CAMPO | FUNCIÓN |
|---|---|
| **Versión** | Son utilizados 4 bits para indicar la versión del IP. La versión actual es la versión 4. La siguiente versión del IP va a ser la versión 6 |
| **Longitud de la Cabecera** | Se utilizan 4 bits que indican el número de palabras de 32 bits en la cabecera IP. La cabecera IP tiene un mínimo de 20 bytes. |
| **Tipo de Servicio** | Se utilizan 8 bits para indicar la calidad del servicio esperado por este datagramas para entrega a través de los encaminadores en la red IP. Especifican procedencia, demora, y tipo de entrega. |
| **Longitud Total** | 16 bits son utilizados para indicar la longitud total incluida cabecera del datagramas IP. |
| **Identificación** | 16 bits son utilizados para identificar este paquete. Si el paquete fuese fragmentado, todos los segmentos que tuviesen esta misma identificación serán usados para reensamblarlos en la maquina destino. |
| **Flags de Fragmentación** | 3 bits son reservados como indicadores del proceso de Sin embargo únicamente 2 bits están definidos para el proceso en curso. Uno de ellos es para indicar cuando el datagrama puede ser fragmentado y el otro para indicar que hay más fragmento que lo siguen. |
| **Offset del Fragmento** | 13 bits se utilizan como un contador del desplazamiento para indicar la posición del fragmento relativo al paquete IP original. Si el paquete no estuviese fragmentado este campo contendrá un cero. |

| | |
|---|---|
| **Tiempo de Vida (TTL)** | 8 bits se utilizan para indicar la cantidad de vida o de 'saltos' que un paquete IP puede realizar antes de ser descartado. |
| **Protocolo** | 8 bits se utilizan como un identificador del protocolo. |
| **Checksum de la Cabecera** | 16 bits son usados como checksum de la cabecera IP únicamente. El cuerpo del mensaje IP no está incluido y deberá ser incluido en él, su propio checksum para evitar errores. |
| **Dirección de Origen** | 32 bits que almacenan la dirección IP del origen. |
| **Dirección de Destino** | 32 bits que almacenan la dirección IP del destino. |
| **Opciones y Relleno** | Un múltiplo de 32 bits es utilizado para almacenar las opciones IP. Si las opciones IP no utilizan los 32 bits, se rellenan con bits adicionales a ceros para que la longitud de la cabecera IP sea un número entero de palabras de 32 bits. |

**Tabla 1-4. Estructura del Paquete IP.**

### 1.4.2. IP en el Router

Cuando un router recibe un paquete, el paquete es pasado a la capa IP la cual realiza lo siguiente:

1. Decrementa el campo TTL (Time to Live) al menos en 1. Puede ser disminuido en una cantidad mayor si el router estuviese congestionado. Si el TTL alcanza el valor de cero, el paquete será descartado.

2. El IP puede fragmentar el paquete en paquetes más pequeños si el paquete fuese demasiado largo para las líneas de salida del router.

3. Si el paquete es fragmentado, el IP crea una nueva cabecera para cada nuevo paquete la cual incluye:

    - Un flag (indicador) de que le siguen nuevos fragmentos.

    - Un número de fragmento (Fragment ID) para identificar todos los fragmentos que continúan.

- Un desplazamiento (Fragment Offset) para permitir que la máquina que lo va a recibir sea capaz de reensamblar el paquete.

4. El IP calcula los nuevos cheksum.

5. El IP obtiene la dirección hardware del siguiente router.

6. Envía el paquete.

En el siguiente host, el paquete subirá en el stack (pila o capa de protocolos) hasta el TCP o el UDP. Este proceso se repite en cada router hasta que el paquete encuentra su destino final. Cuando el paquete llega a su destino final el IP ensamblará las piezas tal y como estaba el paquete original.

### 1.4.3. Direccionamiento IP.

La dirección IP identifica la localización de un sistema en la red. Equivale a una dirección de una calle y número de portal. Es decir, es única. No pueden existir en la misma ciudad dos calles con el mismo nombre y número de portal.

Cada dirección IP tiene dos partes. Una de ellas, identifica a la RED y la otra identifica a la maquina dentro de esa red. Todas las maquinas que pertenecen a la misma red requieren el mismo numero de RED el cual debe ser además único en Internet.

El número de maquina, identifica a una workstation, servidor, router o cualquier dispositivo con soporte TCP/IP conectado a la red. El número de maquina (número de host) debe ser único para esa red. Cada host TCP/IP, por tanto, queda identificado por una dirección IP que debe ser única.

#### Identificación de Red e Identificación de Host.

Hay dos formatos para referirnos a una dirección IP, formato binario y formato decimal con punto. Cada dirección IP es de 32 bits de longitud y está compuesto por 4 campos de 8 bits, llamados bytes u octetos. Estos octetos están separados por puntos y cada uno de ellos representa un número decimal entre cero y 255. Los 32 bits de una dirección IP contienen tanto la identificación de Red como la identificación de hosts dentro de la Red.

La manera más fácil de “leer” para los humanos una dirección IP es mediante la notación decimal con puntos. A continuación un ejemplo de una dirección IP en binario y decimal con punto:

10011001110111000011010100001111 → 153.220.53.15

## 1.5. LIMITACIONES DE IPv4

El Internet logro la transición entre los patrocinadores del gobierno y un ambiente comercialmente conducido por las comunicaciones, algunas de las características originales requieren ser analizada. Por ejemplo, antes del uso comercial del Internet, la seguridad extensa de la comunicación del usuario final no fue requerida. Ahora, tantos los usuarios finales introducen información de su tarjeta de crédito para la realizar comprar y ventas por Internet.

Pero la edición más dramática relacionada con el crecimiento se convirtió en la cantidad enorme de hosts que se conectan a través del Internet, y de las direcciones IP asociadas que eran consumidas por esos hosts. Los analistas de las redes hacen un examen periódico de ambos los hosts y dominios conectados en Internet y han encontrado que esto va aumentando exponencialmente. Con cada uno de esos hosts que se conectan a la red, necesitan una dirección IP única, por lo que esto nos indica cada vez más que se consumen mas direcciones IP. Y aunque el espacio de dirección actual IPv4 puede identificar 4,2 mil millones hosts, la estructura de ese espacio de dirección, dividiéndola en la clase A, la clase B, la clase C, en poco tiempo será un problema. Un mayor crecimiento se compara a un consumo más rápido del espacio de direcciones existente.

Otros problemas relacionados, tales como la jerarquía limitada de las direcciones que es posible dentro de los límites de la dirección de 32 bit en IPv4, más las limitaciones asociadas en el escalamiento de la función de los router (otra vez, el rápido crecimiento de Internet a largo plazo), también fueron identificados.

La anticipación de esta escasez de direcciones IP (con "fecha el pronóstico de la condenación" para el marzo 1994, el tiempo predicho en el cual parte del espacio actual de las direcciones IP sería agotado) forzó a el Internet Engineering Task Force a actuar. En respuesta a estas preocupaciones, en julio de 1991, el IETF comenzó el proceso de investigar el problema, de solicitar las ofertas para las soluciones, y llegar a una conclusión, describiendo este proceso preliminar en RFC 1380, publicado en noviembre de 1992. Además, una nueva área de la investigación, llamó el Internet Protocol Next Generation, o IPng, el IETF fue el encargado de estudiar formalmente estas direcciones.

## 1.6. IPv6 EN INTERNET2

INTERNET2 es una red de investigación y desarrollo (I & D) de alta velocidad que facilita el desarrollo de aplicaciones revolucionarias y su posterior traspaso a la red actual.

Gracias a INTERNET2 se desarrollará unas nuevas generaciones de aplicaciones y redes avanzadas. Para los campos de la educación y la investigación, como medicina de distancia, bibliotecas digitales y laboratorios virtuales.

INTERNET2 no sustituirá a la actual Internet, ni tampoco se ha propuesto como principal objetivo construir una infraestructura paralela. Los participantes tienen enlaces al Internet tradicional para servicios como la web, noticias, correos electrónicos y similares.

Todos aquellos que quieran incorporarse a INTERNET2 deberán cumplir, como mínimo, los siguientes requisitos:

- Pertenecer a alguna universidad, ser miembro de una organización no gubernamental relacionada con el trabajo de redes, o simplemente representar a una corporación interesada en participar en el proyecto desde su nacimiento.

- Los usuarios finales son grupos de investigadores en diversas partes del mundo que desarrollan servicios y aplicaciones que requieren acceso a redes de alta velocidad.

El protocolo de Internet versión 6, conocido por sus siglas IPv6, es el nuevo protocolo que se utilizara en el INTERNET2 y en Internet comercial dentro de los próximos años. Su aplicación se debe a que el reducido espacio de direcciones que ofrece la versión 4 del protocolo de Internet (IPv4) ya esta alcanzando su límite. IPv6 ofrece un número muy superior de direcciones (del orden de 1038) dado que la dirección se representa con 128 Bits (IPv4 32 Bits).

Las redes del INTERNET2 son construidas usando Fibra Óptica, que transporta los datos a la velocidad de la luz. Toda la información que circula por la red recibe la misma prioridad, mientras que gracias a la llamada “Garantía de Calidad de Servicios” QoS (Quality of Service), las aplicaciones podrán solicitar por sí mismas una cantidad determinada de ancho de banda o una prioridad especifica. Gracias a QoS se podrá dar máxima prioridad, por ejemplo, a una videoconferencia con calidad de DVD (Video Digital) para educación a distancia.

# CAPITULO II

# CAPITULO II: EL PROTOCOLO IPv6

## 2.1. EL PUNTO DE REFERENCIA IPv4.

El protocolo de Internet fue desarrollado para "proveer las funciones necesarias para enviar un paquete de bits (un datagramas de Internet) desde una fuente hasta un destino sobre un sistema interconectado de redes", y ha proveído esa función por casi 2 décadas. IP es primariamente concerniente con el envío del datagramas. Igualmente importantes, sin embargo, son las emisiones que IP no direcciona, como el envío puntual de datos de extremo a extremo o el envío de datos secuencial. IP deja estas emisiones para la capa Host-to-Host y las implementaciones del TCP y del UDP que reside allá.

El término datagramas se refiere a un paquete de datos transmitido en una red sin conexión. Sin conexión significa que ninguna conexión entre fuente y destino es establecida antes de la transmisión de datos. La transmisión de datagramas es análoga al envío de una carta. Con ambos, la carta y el datagramas, escribes una dirección fuente y de destinatario en un sobre, pones la información dentro, y pones el paquete dentro de un buzón de correo para su recogida. Pero mientras la oficina de correo utiliza buzones azules o rojos, el Internet usa su nodo de red como el punto de recogida.

Otro tipo de transmisión de datos es una conexión de circuitos virtuales, que usa una red orientada a conexiones. Un circuito virtual es análogo a una llamada telefónica, donde la dirección del destinatario es conectada y un camino es definido a través de una red antes de transmitir datos. IP es un ejemplo de un protocolo basado en datagramas, TCP de un protocolo basado en circuitos virtuales.

En el proceso de entregar datagramas, IP debe negociar con direccionamiento y fragmentación. La dirección asegura que el datagramas llegue al destinatario correcto, sea que esté del otro lado de la ciudad o del otro lado del mundo. La fragmentación es necesaria porque las LAN y WAN que cualquier datagramas atraviese pueden tener tamaños de frames que difieren, y datagramas de IP debe siempre ajustar dentro del frame, como s muestra en la figura siguiente (Por ejemplo, un frame de Ethernet puede acomodar 46 – 1,500 octetos de datos, mientras FDI carga hasta 4,470 octetos). Campos específicos dentro del encabezado de IP manejan las funciones de fragmentación y direccionamiento.

Nótese en la figura 2-1 que cada grupo horizontal de bits (llamado una palabra) es de 32 bits de ancho.

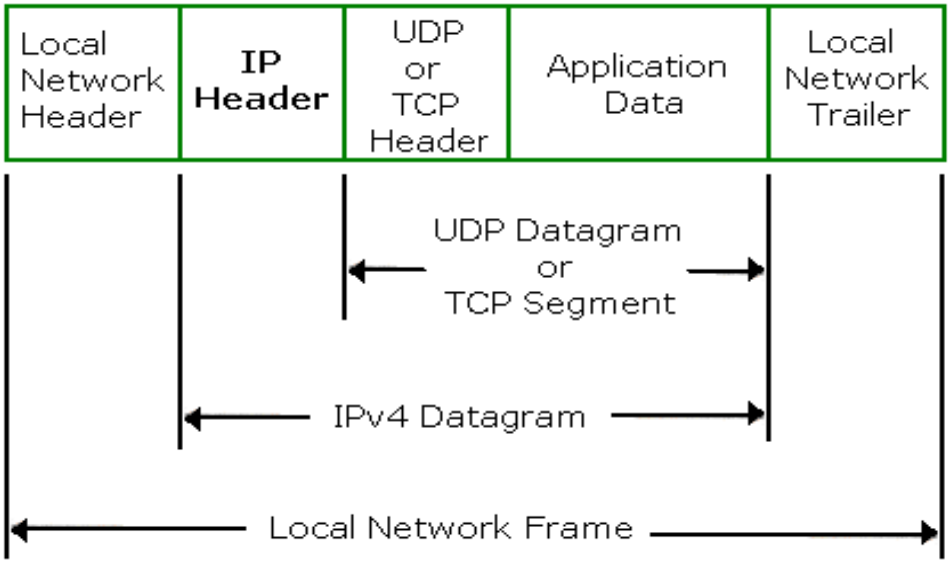



**Fig. 2-1. Dimensiones de un datagramas.**


**Fig. 2-2. Formato De La Cabecera De Un Paquete Ipv4.**

## 2.2. INTRODUCCIÓN A IPv6.

El tremendo crecimiento en el número de usuarios de Internet resultó en que el reconocimiento que el espacio de direcciones de 32 bits del IPv4 tenía una vida

limitada y requería reemplazo. Aunque este reconocimiento ocurrió a final de los 80, no fue sino hasta principio de los 90 en que esta acción tomó lugar.

En una reunión de la Sociedad de Internet en Kobe, Japón, en junio del 1992 había 3 proposiciones para un nuevo IP. Para diciembre del 1992 el número de reemplazo de IP subió a 7 y la IESS (Internet Enginneering Steering Group) organizó un consejo llamado IPNG para repasar las nuevas proposiciones de IP y publicar su recomendación. Esa recomendación se publicó en julio del 1994 en la reunión de Toronto de la IETF y se documento en RFC 1752, The Recommendation for the IP Next Generation Protocol, publicado en enero de 1995. Este nuevo IP es la versión 6 del protocolo de Internet como el IPv5 no pudo ser usado debido a su anterior asignación a un protocolo experimental desarrollado en paralelo al IP y datos en tiempo real. Así, IPNG ahora es conocido como IPv6 en vez de IPv5.

El nacimiento de este nuevo protocolo no ha venido solo propiciado por la escasez de direcciones IPv4 en estos momentos, sino que además se añaden nuevas características y se mejoran las existentes. Sobre IPv4 las tablas de rutas de los routers se están haciendo gigantescas, tanto el multi-homing como la movilidad son tareas excesivamente complejas. Las nuevas necesidades del usuario no pueden ser satisfechas de forma sencilla: seguridad, movilidad y calidad de servicio (QoS) entre otras. De todas estas razones, la única que no tiene alternativa sobre IPv4 es el agotamiento de direcciones: en la práctica las 232 direcciones quedan restringidas a la configuración flexible de las subredes, con lo que el número de direcciones asignado de forma eficiente se nos queda en tan solo 200 millones.

El protocolo IPv4 que forma la Internet de hoy en día está basado en una arquitectura que utiliza direcciones de 32 bits. Con la nueva versión del protocolo, las direcciones constan de 128 bits. Esto significa, entre otras cosas, que soluciones de agotamiento de direcciones IPv4, como el NAT, no serán necesarias. Podemos decir que una “desventaja” de estas nuevas direcciones es su dificultad para recordarlas dado su tamaño: 3ffe:3330:2:0:2a0:c9ff:fe10:cb02 podría ser tranquilamente nuestra dirección IPv6. Es de suponer que el servicio DNS tendrá más importancia aún.

El IPv6 soluciona directamente el problema pendiente de direccionamiento IP con el uso de una dirección de 128 bits que reemplaza las direcciones de 32 bits del IPv4.

Esto resulta en un incremento de espacios de dirección en un factor de 296. En adición a expandir el número de distintas direcciones de IP, los miembros del consejo IPNG simplificaron el encabezado del IP mientras proveen un mecanismo

para mejorar el soporte de una variedad de opciones para incluir esas que pueden solo ser reconocidas como necesarias para ser desarrolladas algunos años desde ahora, añadida la habilidad para etiquetar paquetes pertenecientes a un tipo particular de tráfico por cual el originador solicita manejo especial, y añadido una extensión de encabezado que facilita el soporte de encriptación y autentificación tanto como un encabezado de ruteo cuyo uso podría ser esperado para mejorar el desempeño de la red.

Concerniente al desempeño de la red, uno de los beneficios esperados del IPv6 sobre el IPv4 es en el área de desempeño del router. En el IPv4 las rutas fuentes son codificadas en un campo opcional de encabezado cuyos contenidos deben ser chequeados por todos los routers, aún si ellos no representan un punto de relay específico en la ruta fuente. En comparación, bajo los routers IPv6 son sólo requeridos para examinar los campos destino del encabezado principal del IPv6. Este método de operación requería que el soporte de IPv6 debe cortar los ciclos CPU de routers, habilitando una velocidad de procesamiento de un paquete por segundo (PPS) más alto a ser obtenido bajo condiciones normales de operación.

### 2.2.1. Los criterios para el IPNG.

En diciembre de 1993, el RFC 1550 fue distribuido, titulado "IP: Next Generation (IPng)". Este RFC invitó a cualquier partido interesado que sometiera comentarios con respecto a cualquiera de los requisitos específicos para el IPng o cualquier factor dominante que se deban considerar durante el proceso de selección de IPng. 21 respuestas fueron sometidas que trataron una variedad de asuntos, incluyendo: seguridad (RFC 1674), opinión de un usuario corporativo grande (RFC 1686).

El área de IPng detallado en el RFC 1726, "Criterio Técnico para elegir IP, la nueva generación de direcciones IP (IPng)", para definir los sistemas de los criterios que serían utilizados en el proceso de la evaluación de IPng. Los 18 criterios son los siguientes:

**1- Escalabilidad:** El protocolo de IPng debe permitir la identificación y la dirección de menos 1012 sistemas finales y de 109 redes individuales.

**2- Flexibilidad Topológica:** La arquitectura del encaminamiento y los protocolos de IPng deben permitir muchas diversas topologías de la red.

**3- Funcionamiento:** Los router de categoría normal debe poder procesar y remitir el tráfico de IPng a las velocidades de las cuales son capaces de utilizar, disponible comercialmente, a una velocidad rápida. Los hosts deben poder

alcanzar las tazas de transferencia de datos con IPng que son comparables a las tazas de transferencia alcanzadas con IPv4, usando niveles similares de los recursos del hosts.

**4- Rendimiento:** Deben poder procesar y remitir el tráfico de IPng a las velocidades capaces completamente de utilizar en los medios comercialmente disponibles, a altas velocidades. Los hosts deben poder alcanzar las tazas de transferencia de datos con IPng que son comparables a las tazas de transferencia alcanzadas con IPv4, usando niveles similares de los recursos del hosts.

**5- Servicio Robusto:** El servicio de red y sus protocolos asociados de los encaminamientos y del control deben ser robustos.

**6- Transición:** El protocolo debe tener un plan directo de la transición del IPv4 actual.

**7- Independencia De los Medios:** El protocolo debe trabajar a través una red interna de diversos medios como son LAN, WAN y MAM. Con velocidades individuales de acoplamiento extendiéndose de 1 bits por segundo hasta cientos de gigabits por segundo.

**8- Servicio De datagramas No fiable:** El protocolo debe apoyar un servicio de entrega de datagramas no fiable.

**9- Configuración, administración, y operación:** El protocolo debe permitir la configuración y la operación fáciles y en gran parte distribuida. Se requiere la configuración automática de hosts y de routers.

**10- Operación Segura:** IPng debe proporcionar una capa de red segura.

**11- Nombramiento Único:** IPng debe asignar a cualquier objeto en global, un nombre único en la Capa IP de Internet.

**12- Acceso y documentación:** Los protocolos que definen IPng, sus protocolos asociados, y los protocolos del encaminamiento deben ser publicados en la pista RFCs de los estándares, estar libremente disponibles, y no requerir ningún honorario que licencia para la puesta en práctica.

**13- Multicast:** El protocolo debe permitir transmisiones de paquete unicast y la transmisión del paquete de multicast.

**14- Extensibilidad:** El protocolo debe ser extensible; debe poder desarrollarse para resolver las necesidades futuras del servicio del Internet. Además, como IPng se desarrolla, debe permitir que diversas versiones coexistan en la misma red.

**15- Servicio De Red:** El protocolo debe permitir que la red asocie los paquetes a las clases particulares del servicio y provea de ellas los servicios especificados por esas clases.

**16- Movilidad:** El protocolo debe apoyar los hosts, las redes, y los internetworks móviles.

**17- Protocolo de Control:** El protocolo debe incluir la ayuda elemental para soportar y probar las redes para eliminar los errores.

**18- Redes Privadas:** IPng debe permitir que los usuarios construyan internetworks privados encima de la infraestructura básica del Internet, apoyando internetworks basados en IP y basados en no-IP.

## 2.3. LA CABECERA DE IPv6.

El paquete de IPv6 es cargado en un fame de red local como en IPv4; sin embargo, el encabezado de IPv6 consiste en 2 partes. Estas son el encabezado base de IPv6, más encabezado de extensión opcional. Con o sin algún encabezado de extensión opcional, un constraint de tamaño fijo en uniframe de red local debe ser respetado. Por ejemplo, la mayor cantidad de datos que puede ser cargada en un frame Ethernet es 1500 octetos. Si el encabezado de extensión es añadidos al paquete de IPv6, menos datos de aplicación pueden ser enviados. El host y/o su sistema operativo deben tener un mecanismo para manejar esto.

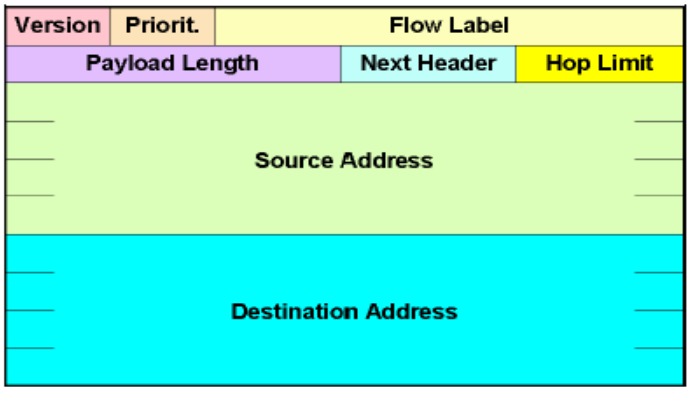



**Fig. 2-3. Formato De La Cabecera De Un Paquete IPv6**

La cabecera de un paquete IPv6 es, sorprendentemente, más sencilla que la del paquete IPv4. Y recordemos que además la funcionalidad del protocolo IPv6 es mucho mayor.

La cabecera de un paquete IPv4 es variable, por lo que necesita un campo de tamaño o longitud. Sin embargo, para simplificar la vida de los enrutadores, IPv6 utiliza un tamaño de cabecera fijo de 40 bytes, que componen un total de ocho campos:

### 2.3.1. El campo Version

El campo Version es de 4 bits de largo e identifica la versión del protocolo.
Para IPv6, Versión = 6. Nótese que este es el único campo con una función y posición que es consistente entre IPv4 e IPv6. Todos los demás son diferentes de alguna forma. El tener este campo al comienzo del paquete permite una rápida identificación de la versión del IP y el paso de ese paquete al protocolo de proceso apropiado: IPv4 o IPv6.

### 2.3.2. El campo Traffic Class

El campo Traffic Class es de 8 bits de largo y su intención para los nodos de origen y/o nodos de reenvío es identificar y distinguir entre diferentes clases o prioridades de paquetes IPv6. (En la primera publicación de la especificación IPv6, RFC 1883, este campo se llamaba Priority, reflejando su función. Mejoras en este trabajo lo renombraron como campo Class, con una longitud de 4 bits.

Trabajo adicional en el IPNG Meeting, en el plenario de agosto 1997 de Munich expandió este campo a 8 bits y redujo el campo Flow Label de 24 bits a 20. El nuevo término Traffic Class, definido en RFC 2460, identifica más el propósito de este campo.)

Este campo reemplaza las funciones que fueron proveídas por el campo Type of Service de IPv4, permitiendo la diferenciación entre categorías del servicio de transferencia de paquetes. Esta función es comúnmente referida como “Servicio de Diferenciación”. Al tiempo de este escrito, algunos experimentos están siendo conducidos en esta área de la tecnología, especialmente en soporte de transporte de señal dependiente del tiempo, como voz o video sobre IP.

Estos 3 requerimientos generales para el campo Traffic Class son stated en RFC 2460:

- Para paquetes que son originados en un nodo por un protocolo de capa más alta, ese protocolo de capa más alta especificaría el valor de los bits del campo Traffic Class. El valor por default es cero.

- Nodos que soportan una función particular que usa bits de Traffic Class pueden cambiar los valores de los bits en paquetes que ellos originan, reenvían o reciban. Sin un nodo no soporta esa función particular, no debe cambiar ninguno de los bits de Traffic Class.

- Los protocolos de capa más alta no deben asumir que los valores de los bits de Traffic Class en un paquete recibido son los mismos valores que fueron originalmente transmitidos. En otras palabras, un nodo intermediario puede ser permitido a cambiar (y haber cambiado) los bits de Traffic Class en tránsito.

Dos de los otros documentos, RFC 2474 y RFC 2475, discuten el concepto e implementación de servicios de diferenciación, que tienen la intención de discriminar entre varios tipos de servicio, requiriendo el estado por carga y señalización en cualquier salto. RFC 2474 define un campo Differentiated Services que reemplaza el campo Type of Service de IPv4. RFC 2475 es más general en la naturaleza, y describe una arquitectura para servicios diferenciados y las funciones a ser proveídas.

Esta arquitectura es descrita en 2 componentes: uno trata con el reenvío de paquetes, y el otro trata con las políticas que determinan los parámetros usados en la ruta de reenvío. Una analogía es dibujada desde las diferencias entre reenvío de paquetes y ruteo de paquetes. El reenvío es el proceso por paquete que determina (de una tabla de ruteo) a qué interfase un paquete debe ser enviado. Rutear es un proceso más complejo que determina las entradas en esa tabla de ruteo, y (posiblemente más importante) la política que determina cómo esa tabla es construida. Como se discutió en RFC 2474, los comportamientos de la ruta de reenvío son mejor entendidos que las políticas que configuran los parámetros que afectan la ruta de envío.

RFC 2474 se concentra en el componente de la ruta de reenvío que determina el comportamiento por saltos (PHB) de los paquetes, más que en la política y parámetros de configuración del componente. Los PHB's incluirían tratamiento específico que un paquete individual recibe, con los elementos del mensaje que son requeridas para que ese tratamiento especial sea eficaz.

Un PHB suficientemente definido debería permitir la construcción de servicios predecibles.

RFC 2474 define el formato para el campo Differentiated Services (DS) que contiene 2 subcampos. El subcampo Differentiated Services Codepoint (DSCP) selecciona el PHB que un paquete experimenta en cada nodo. El campo Currently Used (CU) es reservado para futuras definiciones.

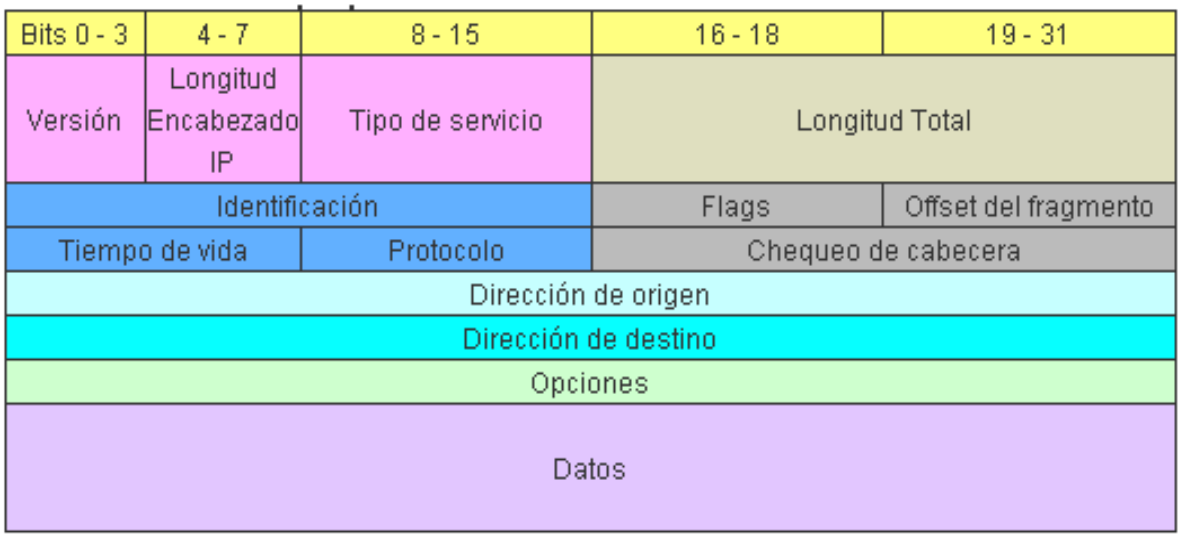



**Fig. 2-4. Estructura Paquete IPv4**

El campo Type of Service de IPv4 consiste en 3 partes: un campo Precedente de 3 bits, 3 bits que especifican banderas (Delay, Throughput y Reliability, o DTR) y 2 bits que son reservados. RFC 2474 define un grupo de puntos de código, el patrón de bits para el subcampo DSCP sería XXX000 (en binario, donde x sería cero o uno). Nótese que los 3 "X" bits corresponden con las mismas posiciones de los bits de DTR; sin embargo, RFC 2474 establece que ningún atento es hecho para mantener compatibilidad hacia atrás con esos bits de banderas. También, el punto de código con valor 000000 es asignado al PHB por default, que es definido como el comportamiento de envío "común, de más esfuerzo". (Nótese la comparación con el campo de precedencia, éste correspondería con el valor para precedencia de "rutina".)

Otros valores de punto de código han sido agrupados en pools, con un pool reservado para tareas basadas en estándares, y otros, para propósitos de uso local y experimental. RFC 2474 describe estas tareas en detalle más grande.

### 2.3.3. El Campo Flow Label

El campo Flow Label es de 20 bits de longitud, y puede ser usado por un host para solicitar manejo especial para ciertos paquetes, como aquellos con una calidad de servicio de no default o de tiempo real. En esta primera versión de la especificación IPv6, RFC 1883, este campo era de 24 bits de longitud, pero 4 de estos bits han sido ahora colocados en el campo Traffic Class, como se discutió en la sección anterior.

Un flujo es una secuencia de paquetes enviados a un destino unicast o multicast que necesita manejo especial por los routers IPv6 que intervienen.

Todos los paquetes pertenecientes a un mismo flujo debe ser enviado con la misma dirección fuente, dirección destino y etiqueta de flujo. Un ejemplo de un flujo sería paquetes que soportan un servicio en tiempo real, como audio o vídeo.

Flow Label es usado por esa fuente para etiquetar esos paquetes que requieren manejo especial por el nodo IPv6. Si un host o router no soporta funciones de Flow Label, el campo es fijado a cero en el origen e ignorado en la recepción.

Múltiples flujos de datos pueden existir entre una fuente y un destino, así como tráfico de datos que no es asociado con un flujo particular. Un flujo único es identificado por la combinación de una dirección fuente y una etiqueta de flujo que no sea cero. La etiqueta de flujo es un número seudo-aleatorio elegido del rango de 1 a FFFFFH (donde H denota notación hexadecimal). Esa etiqueta es usada como una clave hash por router para buscar el estado asociado con ese flujo.

RFC 1809, “Usando el Campo Flow Label en IPv6”, describe algunas de las investigaciones más tempranas en la materia, como el campo Class, Flor Label es sujeto de investigación actualmente y puede cambiar según la experiencia de la industria madura.

### 2.3.4. El campo Payload Field

El campo Payload Field es un entero no asignado de 16 bits que mide la longitud, dada en octetos, de la carga (ejemplo el balance del paquete IPv6 que sigue al encabezado base de IPv6). Nótese que los encabezados de extensión opcional son considerados parte de la carga, junto con cualquier protocolo de capa más alta, como TCP, FTP y así.

El campo Payload Length es similar al campo Total Length de IPv4, excepto que las 2 medidas operan en diferentes campos. Payload Length (IPv6) mide los datos

después del encabezado, mientras Total Length (IPv4) mide los datos y el encabezado.

Las cargas más grandes de 65,535 son permitidas y son llamadas Cargas Jumbo. Para indicar una carga jumbo, el valor de Payload Length está fijado en cero y la longitud de la carga actual es especificada en una opción que es cargada en la extensión del encabezado Hop-by-Hop.

### 2.3.5. El Campo de Siguiente Cabecera (Next Header Field)

El campo Next Header tiene 8 bits de longitud e identifica el encabezado inmediatamente siguiente del encabezado de IPv6. Este campo usa los mismos valores que el campo Protocol de IPv4. Ejemplos:

| Value | Header |
|---|---|
| 0 | Hop-by-Hop Options |
| 1 | ICMPv4 |
| 4 | P in IP (encapsulation) |
| 6 | TCP |
| 17 | UDP |
| 43 | Routing |
| 44 | Fragment |
| 50 | Encapsulating Security Payload |
| 51 | Authentication |
| 58 | ICMPv6 |
| 59 | None (No Next Header) |
| 60 | Destination Options |

**Tabla 2-1. Valores del Campo de Siguiente Cabecera.**

Un paquete IPv6, que consiste en un paquete de encabezado IPv6 más su carga, puede consistir de cero, uno o más encabezados de extensión. Muchos de los encabezados de extensión también emplean un campo Next Header.

Nótese los valores de los campos Next Header en cada ejemplo mostrado en la figura. En el primer caso ningún encabezado de extensión es requerido, Next

Header = TCP, y el encabezado TCP y cualquier protocolo de capa más alta le sigue. En el segundo ejemplo, un header Routing es requerido. Luego, Next Header de IPv6 = Routing; en el header Routing, Next Header = TCP, y el encabezado TCP y cualquier protocolo de capa más alta le sigue. En el tercer caso, tanto el header Routing como Fragment son requeridos, con los campos Next Header identificados acordemente.

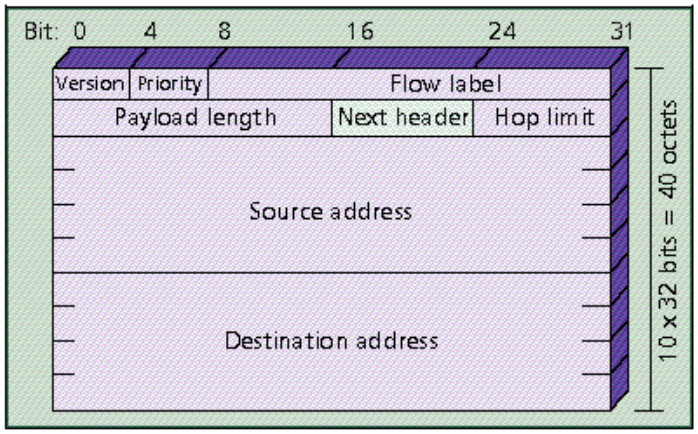



**Fig. 2-5. Dimensiones de La Cabecera de IPv6**

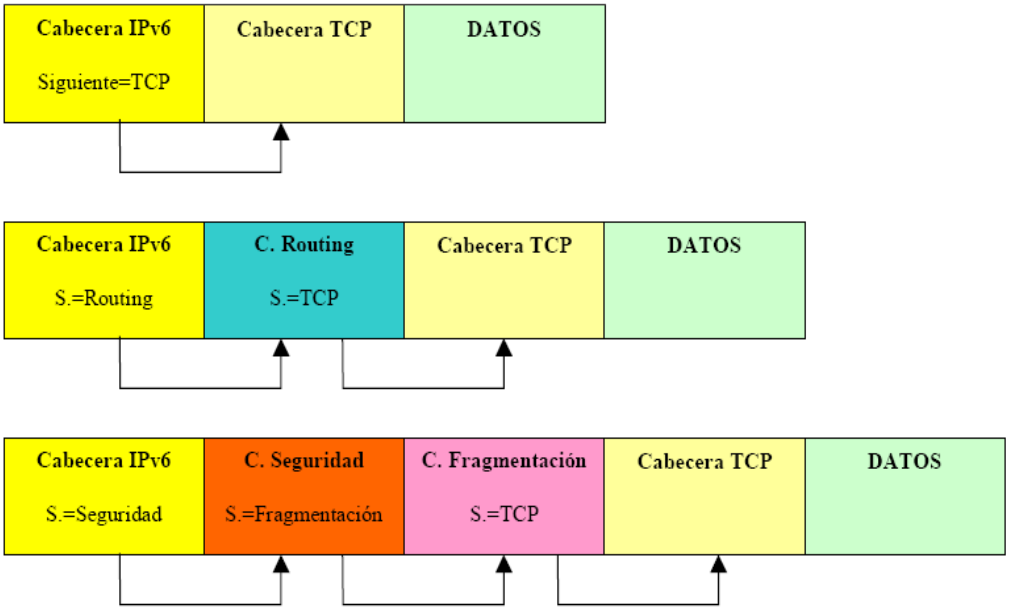



**Fig. 2-6. Funcionamiento del Campo de Siguiente Cabecera.**

### 2.3.6. El campo Hop Limit

El campo Hop Limit tiene 8 bits de longitud, y va descreciendo en 1 por cada nodo que reenvía el paquete. Cuando Hop Limit se iguala a cero, el paquete es descartado y un mensaje de error es retornado. Este campo es similar al campo Time-to-Live (TTL) encontrado en IPv4, con una excepción clave. El campo Hop Limit (IPv6) mide el máximo de saltos (hops) que pueden ocurrir mientras el paquete es enviado por varios nodos. El campo TTL (IPv4) puede ser medido en saltos o segundos. Notese que con Hop Limit usada en IPv6, la base del tiempo no está disponible más.

### 2.3.7. El campo Source Address

El campo Source Address es un campo de 128 bits que identifica el productor del paquete. El formato de este campo es más ampliamente definido en RFC 2373.

### 2.3.8. El campo Destination Address

El campo Destination Address es un campo de 128 bits que identifica el destinatario que tiene la intención de recibir el paquete. Una importante distinción es la de que el destinatario que tiene la intención de recibir el paquete puede no ser el destinatario final, como el header Routing puede ser empleado para especificar la ruta que el paquete toma desde su fuente, a través de destinatario(s) intermedio(s), y así hasta su destinatario final.

## 2.4. ENCABEZADOS DE EXTENSIÓN

El diseño de IPv6 simplifica el encabezado existente de IPv4 colocando muchos de los campos existentes en encabezado opcionales. De esta forma, el procesamiento de paquetes ordinarios no es complicado por uso indebido de encabezados, mientras las condiciones más complejas son todavía proveídas.

Como hemos visto, un paquete IPv6, que consiste de un paquete IPv6 más su carga, puede consistir de cero, uno o más encabezados de extensión. Cada encabezado de extensión es un múltiple integral de 8 octetos de longitud para retener la alineación de 8 octetos para encabezados subsecuentes. Para óptimo desempeño del protocolo, estos encabezados de extensión son colocados en un orden específico.

### 2.4.1. Orden de los Encabezados de Extensión

RFC 2460 recomienda que los encabezados de extensión sean colocados en el paquete IPv6 en un orden particular:

- IPv6 Header.
- Hop-by-Hop Options Header.
- Destination Options Header (para opciones a ser procesadas por el primer destino que aparece en el campo Destination Address de IPv6, más destinos subsecuentes listados en el Routing Header).
- Routing Header.
- Fragment Header.
- Authentification Header (como se detalla en RFC 2402).
- Encapsulating Security Payload Header (como se detalla en RFC 2406).
- Destination Options Header (para opciones a ser procesadas por el destino final solamente).
- Upper Layer Protocol Header (TCP, etc.).

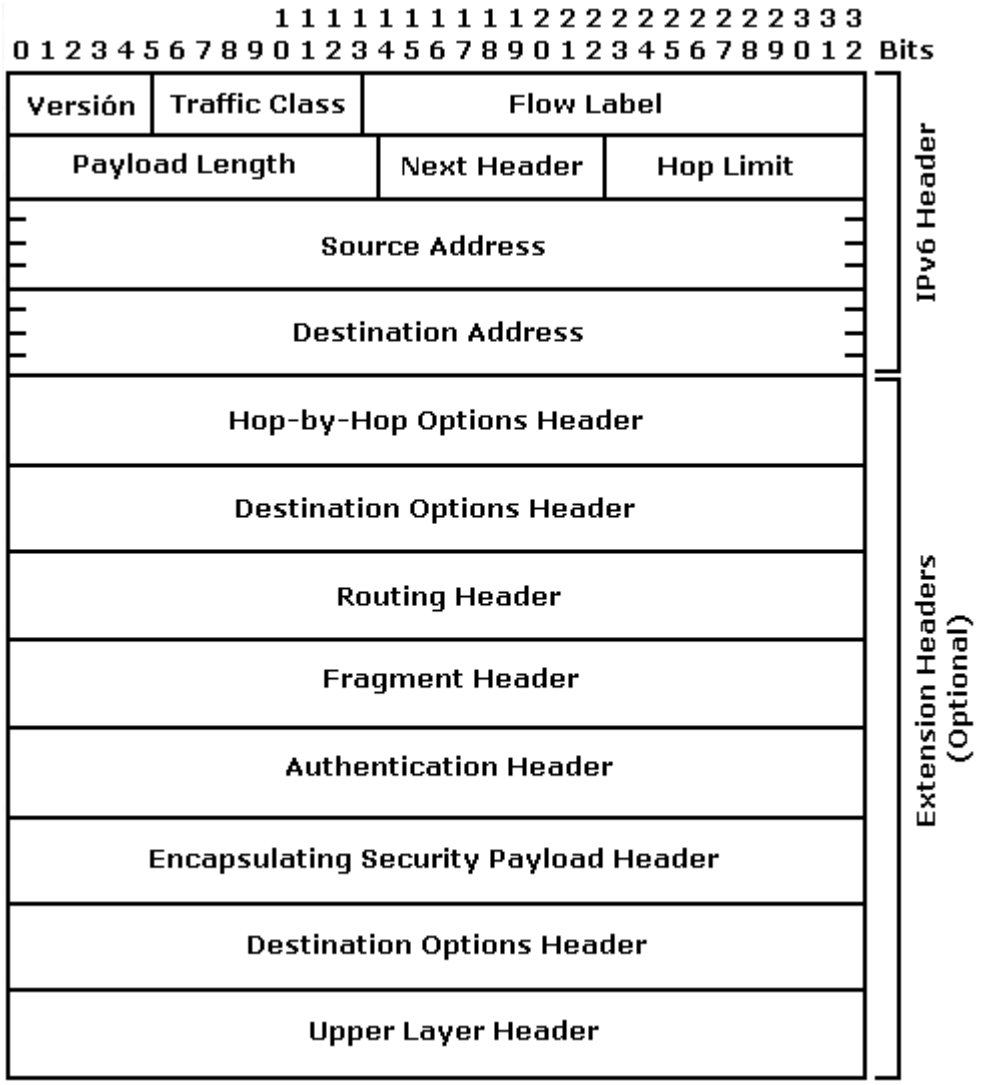



**Fig. 2-7. Orden de los Encabezados de Extensión.**

### 2.4.2. Opciones de los Encabezados de Extensión

Dos de los encabezados de extensión, Hop-by-Hop y Destination Options, pueden cargar una o más opciones que identifican más allá de los parámetros de operación de red. Estas opciones son codificadas usando el formato TLV (Tipo-Longitud -Valor) que es especificado por el lenguaje de descripción de mensajes Abstract Syntax Notation 1 (ASN.1) (TLV es ampliamente usado entre protocolos de comunicación, incluyendo el Simple Network Management Protocol, SNMP.) La

opción formato incluye un campo Option Type de 8 bits que identifica la longitud del campo Option Data dada en octetos; y un campo Option Data de longitud variable.

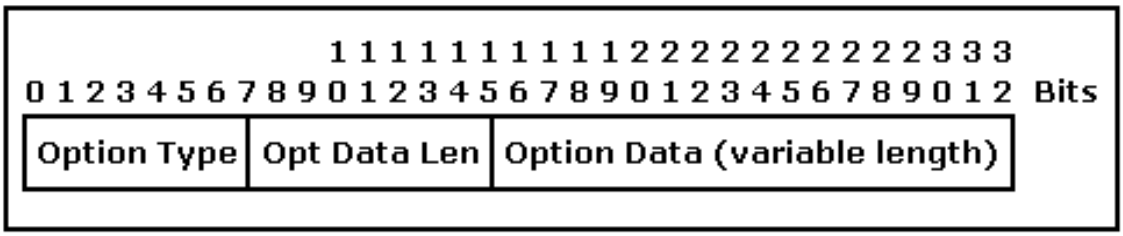



**Fig. 2-8. Opciones de los Encabezados de Extensión.**

Los dos bits de orden más alto del Campo Option Type, especifican como tener opciones que son irreconocibles en el nodo de procesamiento de IPv6:

| Valor | Acción |
|---|---|
| OO | Salta la opción y continúa procesando el encabezado. |
| O1 | Descarta el paquete. |
| 1O | Descarta el paquete y envía un mensaje ICMP Problema de Parámetro (Tipo de Opción irreconocible) a la fuente. |
| 11 | Descarta el paquete y envía un mensaje ICMP problema de parámetro (Tipo de Opción irreconocible) a la fuente (solo si el destino no era multicast). |

**Tabla 2-2. Los 2 bits de orden más alto del Campo Option Type.**

El tercer BIT de orden más alto del campo Option Type especifica si Option Data de esa opción puede cambiar en ruta al destino final del paquete o no.

| Valor | Acción |
|---|---|
| 0 | Option data no cambia su valor en ruta |
| 1 | Option data puede cambiar su valor en ruta |

**Tabla 2-3. Tercer bit de orden más alto.**

Además, hay 2 opciones que son usadas, como necesarios, para rellenar las opciones de forma que el encabezado de extensión contenga un múltiplo de 8 octetos. Pad1 Option es usado para insertar 1 octeto de relleno en el área de opciones en el encabezado. Nótese que esta opción es un caso especial (notado por Type = 0) que no tiene los campos Opt Data Len ó Option Data.

PadN Option es usada para insertar 2 ó más octetos de relleno en el área Options de un encabezado. Nótese que esta opción tiene un campo Type = 1. Si el relleno deseado fuera n octetos, el campo Opt Data Len contendría el valor n-2 octetos de valor cero.

### 2.4.3. Encabezado de Extensión Hop-by-Hop

El encabezado de opción Hop-by-Hop carga información opcional que debe ser examinada por cada nodo dentro de la ruta de envío del paquete. Como resultado, el encabezado de opción Hop-by-Hop, cuando está presente, debe inmediatamente seguir al encabezado de IPv6. (Los otros encabezados de extensión no son examinados o procesados por ningún nodo en la ruta de envío del paquete hasta que el mismo alcanza su destino(s) propuesto(s).) La presencia del encabezado Hop-by-Hop es identificada por un valor de 0 en el campo Next Header del encabezado IPv6. Este encabezado posee 2 campos, más opciones.

El campo Next Header tiene 8 bits de longitud, e identifica el encabezado que inmediatamente continúa el encabezado de opción Hop-by-Hop. Este campo usa los mismos valores que el campo Protocol de IPv4.

El campo Header Extension Length (Hdr Ext Len) tiene 8 bits de longitud, y mide la longitud del encabezado Hop-by-Hop Options en unidades de 8 octetos, sin contar los primeros 8 octetos.

El campo Options es variable en longitud, siempre que el encabezado Hop- by-Hop Options completo sea un entero y un múltiplo de 8 octetos de longitud.

Una opción actualmente definida, la opción Jumbo Payload, que es usada para enviar paquetes de IP que son entre 65,536 y 4, 294, 967,295 octetos de longitud. Esta opción es definida por Option Type = 194 (o C2H), Opt Data Len = 4 (octetos) y un campo de 4 octetos que carga la longitud del paquete jumbo en octetos (excluyendo el encabezado base de IPv6, pero incluyendo el encabezado Hop-by-Hop Options y algún otro encabezado). Jumbo Payload Length debe ser más grande que 65,535. También, el campo Payload Length = 0 (para indicar una condición especial) cuando Jumbo Payload es usado.

### 2.4.4. Encabezado Destination Options

El encabezado Destination Options carga información que debe ser examinada solo por el (los) nodo(s) destino(s) del paquete. La presencia del encabezado Destination Options es identificada por un valor de 60 en el campo Next Header del encabezado precedente. Este encabezado contiene 2 campos más opciones.

El campo encabezado Extension Length (Hdr Ext Len) tiene 8 bits de longitud, mide la longitud del encabezado Destination Options en unidades de 8 octetos, sin contar los primeros 8 octetos.

El campo Options es variable en longitud, como el encabezado Destination Options, es un entero múltiple de 8 octetos de longitud. Solo 2 opciones son definidas en RFC 2460 – la opción Pad1, usada para insertar 1 octeto de relleno en el área Options de un encabezado, y PadN, usada para insertar 2 ó más octetos de relleno en el área Options de un encabezado.

### 2.4.5. Encabezado Routing

El header Routing lista uno o más nodos intermediarios que son “visitados” en la ruta desde la fuente hasta el destino. La presencia del encabezado Routing es identificada por un valor de 43 en el campo Next Header del encabezado precedente. Este encabezado contiene 4 campos, más data de tipo específico.

El campo Next Header tiene 8 bits de longitud, e identifica el encabezado que continúa inmediatamente al encabezado Routing. Este campo usa los mismos valores que el campo Protocol de IPv4.

El campo Header Extension Length (Hdr Ext Len) tiene 8 bits de longitud, y mide la longitud del encabezado Routing en unidades de 8 octetos, sin contar los primeros 8 octetos.

El campo Routing Type tiene 8 bits de longitud e identifica una variante particular del encabezado Routing. (RFC 2460 define una variante, Routing Type 0, que es descrita debajo).

El campo Segments Left tiene 8 bits de longitud, e indica el número de segmentos de ruta que quedan, o en otras palabras, el número de nodos intermedios explícitamente listados que todavía serán visitados antes de alcanzar el destino final.

El campo Type-Specific es variable en longitud, con un formato definido por la variante particular Routing Type.

RFC 2460 define una variante simple, el encabezado Routing Type 0, que contiene una lista ordenada de direcciones que serán visitadas durante la ruta del paquete. Para este encabezado, el campo Next Header es definido como arriba; sin embargo, el campo Hdr Ext Len contiene un número igual a 2 veces el número de direcciones en el encabezado. Por ejemplo, si hubiese n direcciones en el encabezado, el campo Hdr Ext Len contendría el valor 2n. El campo Routing Type indicaría Type = 0. El campo Segments Left sería como arriba, y el campo Reserved sería configurado a cero para la transmisión e ignorado en la recepción. Una lista de direcciones de 128 bits, numerada de 1 a n, completaría el header Routing Type 0.

RFC 2460 da un ejemplo del uso del header Routing. En este ejemplo, Nótese que los 3 nodos intermediarios (y cuatro segmentos) separan el nodo Fuente (S) del nodo Destino (D).

Para viajar del nodo Fuente al nodo Intermediario I (I1), el encabezado base de IPv6 usa Source Address (SA) = S, y Destination Address (DA) = I1. El encabezado Routing especifica un Hdr Ext Len (HEL) = 6, Segments Left = 3, y las direcciones de los 3 nodos restantes durante el camino: nodo Intermediario 2 (I2), nodo Intermediario 3 (I3) y nodo Destino (D).

Para viajar de I1 a I2, el algoritmo de ruteo intercambia la dirección Destino de IPv6 con la primera dirección en la lista de direcciones (I2). Nótese que Source Address (SA = S) será consistente para todos los segmentos.

Para viajar de I2 a I3, el algoritmo de ruteo intercambia la dirección Destino de IPv6 con la segunda dirección en la lista de direcciones (I3).

Para viajar de I3 al Destino final (D), el algoritmo de ruteo intercambia la dirección Destino de IPv6 con la tercera dirección en la lista de direcciones (D).

Nótese que el estado final de las direcciones de encabezado de IPv6 es ahora SA = S y DA = D, y el encabezado Routing lista los nodos intermediarios, I1, I2 e I3, en el orden en que fueron visitados.

### 2.4.6. Encabezado Fragment

El encabezado Fragment es usado por una fuente IPv6 para transmitir paquetes que son más grandes de lo que cabrían en la unidad de transmisión máxima (MTU) del paquete a sus destinos. La presencia del encabezado Fragment es identificada por un valor de 44 en el campo Next Header en el encabezado precedente. Nótese que la fragmentación para IPv6 es sólo hecha en el nodo fuente, no en los routers intermediarios junto a la ruta de envío del paquete; este es un cambio de procedimiento desde IPv4.

El encabezado Fragment contiene 6 campos. El campo Next Header tiene 8 bits de largo e identifica el encabezado que continúa inmediatamente al header Fragment. Este campo tiene los mismos valores que el campo del Protocolo IPv4.

El campo Reserved tiene 8 bits de largo, y está reservado para uso futuro. Este campo es inicializado en cero para la transmisión e ignorado en la recepción.

El campo Fragment Offset es un entero sin signo de 13 bits que mide la compensación, en unidades de 8 octetos, de los datos que continúan este encabezado, relativo al comienzo de la parte fragmentable del paquete original.

El campo reservado tiene 2 bits de largo, y está reservado para uso futuro. Este campo es inicializado en cero para la transmisión e ignorado en la recepción.

La bandera M es de 1 bit de longitud y determina si más fragmentos vienen (M = 1) o si este es el último fragmento (M = 0).

El campo Identification es de 32 bits de largo y únicamente identifica el (los) paquete(s) fragmentado(s) durante el proceso de re-ensamblaje. Este campo es generado por el nodo fuente.

Un paquete requiriendo fragmentación es considerado que consiste de 2 partes: una parte no fragmentable y una parte fragmentable. La parte no fragmentable incluye el encabezado IPv6, más cualquier encabezado de extensión que debe ser procesado en ruta al destino. Este puede incluir un encabezado Hop-by-Hop y un encabezado Routing. La parte fragmentable es el balance del paquete, que puede incluir cualquier encabezado de extensión que es procesado al final del nodo destino, los encabezado de capa más alta, y datos de aplicación.

La parte fragmentable del paquete original está dividida en fragmentos que son íntegros múltiplos de 8 octetos (excepto tal vez por el último fragmento, que puede no ser un íntegro múltiplo de 8 octetos). Cada paquete fragmentado consiste de 3 partes: la parte no fragmentable del paquete original, un encabezado Fragment y un fragmento de datos. La parte no fragmentable de cada fragmento contiene un campo Payload Length revisado (con la porción de IPv6) que hace juego con la longitud de este fragmento y un campo Next Header = 44 (indicando que un encabezado Fragment viene después).

Las longitudes de los fragmentos resultantes caben dentro del MTU de la ruta a los destinos de los paquetes. En el(los) nodo(s) destino(s), un proceso llamado re-ensamblaje es usado para reconstruir el paquete original de los paquetes fragmentados. El proceso de reensamblaje es también descrito en RFC 2460.

### 2.4.7. Encabezado de Autentificación

Asegurando las transmisiones de datos se ha convertido en un tema extremadamente importante para los manejadores de red. La comunidad de Internet ha direccionado estos temas en RFC 2401 “Security Architecture for the Internet Protocol”. En el capítulo 7 se discutirá esta arquitectura en detalle.

Dos encabezado son discutidos en RFC 2401 que proveen los mecanismos de seguridad de IP. El encabezado Authentification es definido en RFC 2402.
Encapsulating Security Payload (ESP) es definido en RFC 2406. Estos dos mecanismos pueden ser usados separadamente, o conjuntamente, como las necesidades de seguridad lo dicten.

El encabezado Authentification provee integridad sin conexiones y autentificación de datos de origen para datagramas de IP, más protección original contra “replays”. La presencia de este encabezado es identificada por un valor de 51 en el campo Next Header en el encabezado precedente. Este encabezado contiene 6 campos.

El campo Next Header tiene 8 bits de largo e identifica el encabezado que continúa inmediatamente al encabezado Authentification. Este campo usa los mismos valores que el campo del Protocolo IPv4.

El campo Payload Length tiene 8 bits de longitud y provee la longitud del encabezado Authentification en palabras de 32 bits, menos 2 (ejemplo: los primeros 8 octetos del encabezado Authentification no son contados). El valor mínimo es 1, que consiste en el valor de autentificación de 96 bits (3 palabras de

32 bits), menos el valor 2 (3 – 2 = 1). Este mínimo es sólo usado en el caso de un algoritmo de autentificación “nulo”, empleado para procesos de depuración.

Los campos reservados tienen 16 bits de longitud y es reservado para uso futuro. Este campo es inicializado en cero para la transmisión. Está incluido en cálculo Authentification Data, pero sino es ignorado en la recepción.

El campo Security Parameters Index (SPI) es un valor arbitrario de 32 bits que identifica la asociación de seguridad (SA) para este datagramas, relativo a la dirección contenida en el encabezado de IP al que este encabezado de seguridad es asociado, y relativo al protocolo de seguridad empleado. La asociación de seguridad, como se define en RFC 2401, es una conexión simple y lógica que es creada para propósitos de seguridad. Todo tráfico que atraviesa SA tiene el mismo proceso de seguridad. SA puede comprimir muchos parámetros, incluyendo el algoritmo Authentification, claves del algoritmo de autentificación y otros. Según RFC 2402, el valor de SPI = 0 puede ser usado para propósitos locales, de implementación específicas. Otros valores, en el rango de 1 – 255, son reservados para uso futuro por la Internet Assigned Numbers Authority (IANA).

El campo Sequence Number contiene un número de 32 bits que aumenta “monotónicamente”. Tanto el contador del que envía como el contador del que recibe son inicializados en cero cuando una asociación de seguridad es establecida.

Authentification Data es un campo de longitud variable que contiene el Valor de Chequeo de Integridad - Integrity Check Value (ICV). Este campo debe ser un múltiplo integral de 32 bits de longitud.

### 2.4.8. Encabezado Encapsulating Security Payload

El encabezado propuesto Encapsulating Security Payload (ESP) está designado para proveer confidencialidad, autentificación de datos de origen, integridad sin conexión, un servicio anti-“replay”, y confidencialidad de flujo limitado de tráfico. El(los) servicio(s) proveído(s) depende de la asociación de seguridad y su implementación. La presencia del encabezado ESP es identificada por un valor de 50 en el campo Next Header del encabezado precedente. Este encabezado contiene 7 campos, algunos obligatorios, otros opcionales dependiendo de la asociación de seguridad.

El campo Security Parameters Index (SPI) es un valor arbitrario de 32 bits que identifica la asociación de seguridad para este datagramas, relativo a la dirección IP destino contenido en el encabezado IP con el que este encabezado de

seguridad es asociado, y relativo al protocolo de seguridad empleado. El campo SPI es obligatorio.

El campo Sequence Number contiene un número de 32 bits que "monotónicamente" aumenta. El contador del que envía y el contador del que recibe son inicializados en cero cuando una asociación de seguridad es establecida. El campo Sequence Number es obligatorio.

El campo Payload Data es de longitud variable que contiene datos descritos por el campo Next Header. El campo Payload Data es obligatorio.

El campo Padding puede opcionalmente contener 0 – 255 octetos de información de relleno, como requerido por la implementación de seguridad. El campo Pad Length indica el número de octetos de relleno (0 – 255) que son inmediatamente precedidos.

El campo Padding es obligatorio. El campo Next Header tiene 8 bits de largo e identifica el encabezado que inmediatamente continúa al encabezado ESP. Este campo tiene los mismos valores que el campo del protocolo de IPv4. El campo Next Header es obligatorio.

Authentification Data es un campo de longitud variable que contiene un Valor de Chequeo de Integridad - Integrity Check Value (ICV). La longitud de este campo depende de la función de autentificación que es seleccionada. El campo Authentification Data es opcional, y es incluido sólo si esa asociación de seguridad ha seleccionado servicio de autentificación.

### 2.4.9. Encabezado No Next

El valor de 59 en el campo Next Header de un paquete de IPv6 o cualquiera de los encabezados de extensión indica que nada continúa a ese encabezado.
Por esto, éste se llama "No Next".

# CAPITULO III

# CAPITULO III: ARQUITECTURA DE DIRECCIONAMIENTO

Sin interrogantes, el desarrollo más dramático proveído por IPv6 es el aumento del tamaño en el campo de direcciones – de 32 a 128 bits por dirección. Mientras el campo de 32 bits de IPv4 produce 4, 294, 967,296 direcciones distintas, el campo de 128 bits de IPv6 tiene considerablemente más:

340,282,366,920,938,463,374,607,431,768,211,456 en total. Ha sido estimado que esto iguala a 32 direcciones por pulgada cuadrada de tierra seca en la superficie de la Tierra.

Pero antes de estudiar esta estructura de direccionamiento y todos sus rigores, se deben considerar brevemente los formatos de direccionamiento de IPv4 para comparación.

## 3.1. MODELOS DE DIRECCIONAMIENTO.

Cualquier tipo de dirección se asigna a interfaces, no nodos. Es algo importante que no haya que olvidar. Todas las interfaces han de tener, por los menos, una dirección de enlace local (Link -Local) de tipo unicast. Un mismo interfaz puede tener asignadas múltiples direcciones de cualquier tipo (unicast, anycast, multicast) o ámbito (scope). Direcciones unicast con ámbito mayor que el de enlace no son necesarias para interfaces que no son usados como origen y destino de paquetes IPv6 hacia o desde no vecinos. Esto significa que para la comunicación dentro de una LAN no nos hacen falta direcciones IPv6 globales, sino que tenemos más que suficiente con direcciones de ámbito local. De hecho, es lo aconsejable para enlaces punto a punto.

Respecto a los prefijos de subred, IPv6 sigue el mismo modelo que IPv4, es decir, un prefijo se asocia a un enlace, pudiendo haber varios prefijos en un mismo enlace.

La estructura de dirección IPv6 encuentra sus raíces en la estructura CIDR, que incluye un prefijo de dirección, un ID de Site y un ID de Host. Para IPv6, sin embargo, habrá múltiples prefijos de direcciones, y cada uno de ellos puede tener múltiples estructuras similares a ID de Site y ID de Host. Como una base, el documento de arquitectura de direccionamiento de IPv6, define 3 tipos diferentes de direcciones IPv6:

- **Unicast:** Un identificador para una interfase simple. Un paquete enviado a una dirección unicast es entregado a la interfase identificada por esa dirección.

- **Anycast:** Un identificador para un conjunto de interfases (típicamente perteneciente a nodos diferentes). Un paquete enviado a una dirección anycast es entregado por una de las interfases identificadas por esta dirección (la más cercana, según la medida de distancia del protocolo de ruteo).

- **Multicast:** Un identificador para un conjunto de interfases (típicamente perteneciendo a nodos diferentes). Un paquete enviado a una dirección multicast es entregado a todas las interfases identificadas por esta dirección.

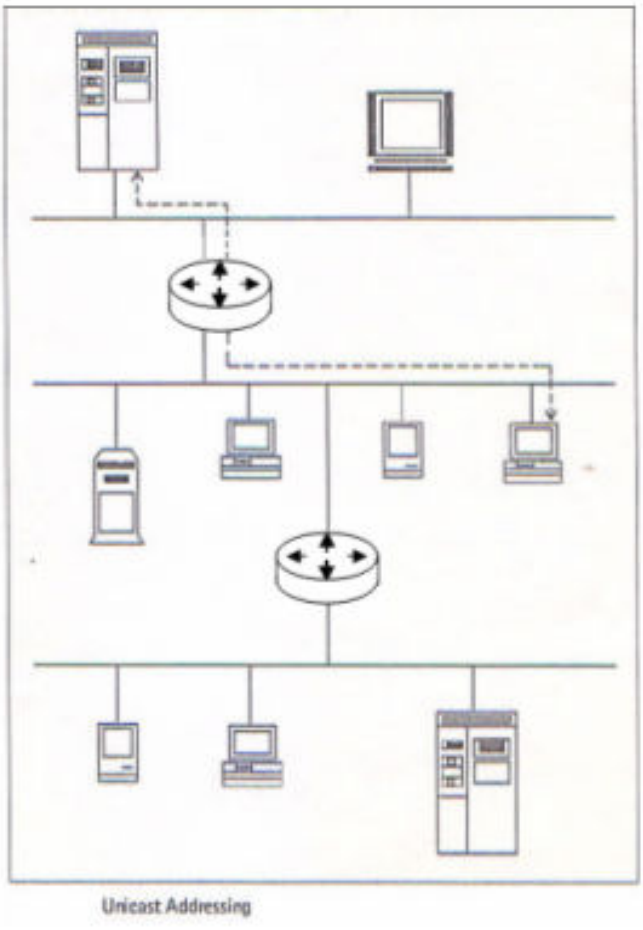



**Fig. 3-1. Direccionamiento Unicast**

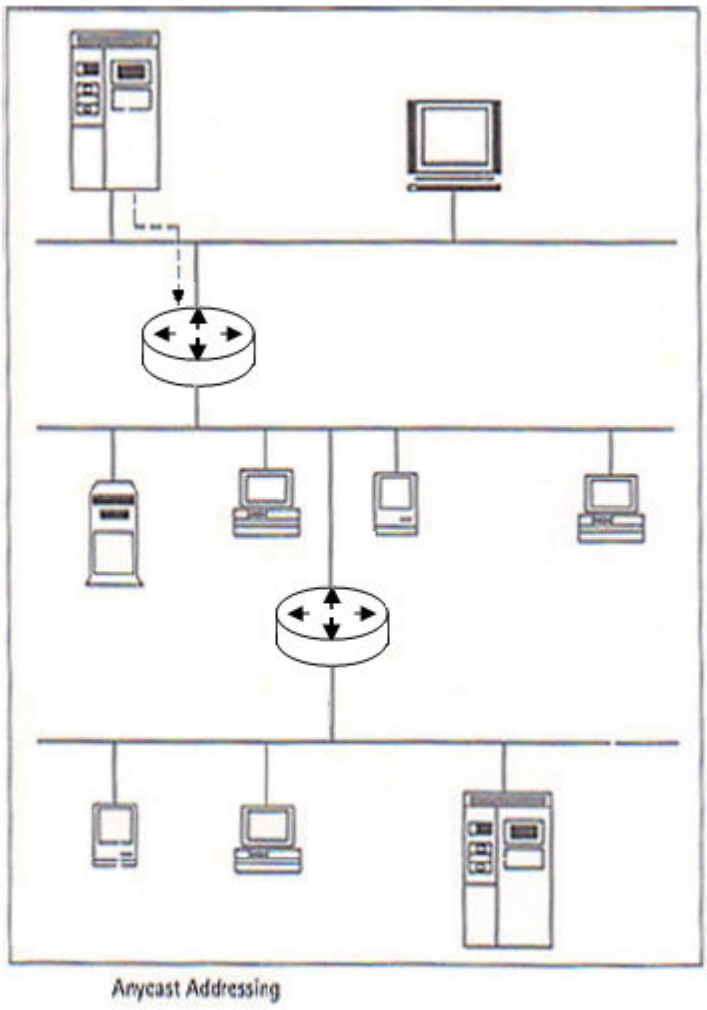



**Fig. 3-2. Direccionamiento Anycast**

Nótese que el término difusión (broadcast) no aparece, porque la función de difusión es reemplazada por la definición de multicast. También Nótese que las direcciones de IPv6 de todo tipo son asignadas a interfases, no nodos; un nodo (como un router) puede tener múltiples interfases, y así múltiples direcciones unicast. Además, una interfase simple puede estar asignada a múltiples direcciones.

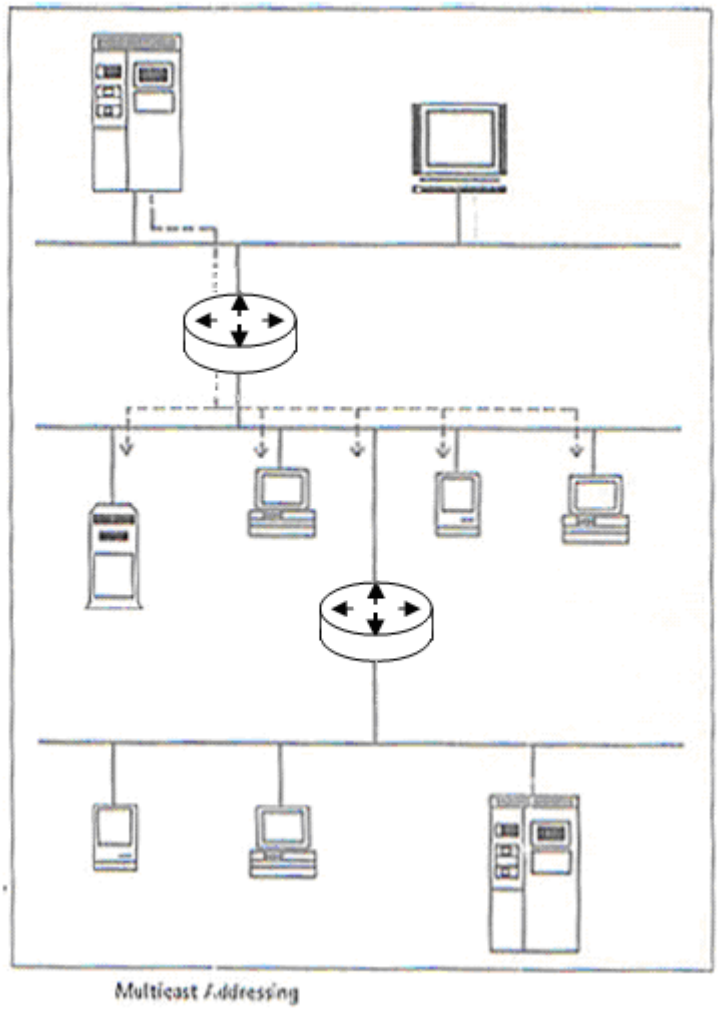



**Fig. 3-3. Direccionamiento Multicast.**

## 3.2. ÁMBITOS.

El protocolo IPv6 añade soporte para direcciones de distintos ámbitos, lo que quiere decir que se tendrán direcciones globales y no globales. Si bien con IPv4 ya se había empleado direccionamiento no global con la ayuda de prefijos de red privados, con IPv6 esta noción forma parte de la propia arquitectura de direccionamiento.

Cada dirección IPv6 tiene un ámbito, que es un área dentro de la cual esta puede ser utilizada como identificador única de uno o varias interfaces. El ámbito de cada

dirección forma parte de la misma dirección, con lo que se podrán diferenciar a simple vista.

Para las direcciones unicast se distinguen tres ámbitos:

- De enlace local (link-local), para identificar interfaces en un mismo enlace. Empiezan todas por **fe80:.**

- De sitio local (site-local), para identificar interfaces en un mismo 'sitio'. La definición de 'sitio' es un tanto genérica, pero en principio un 'sitio' es el área topológica de red perteneciente a un edificio o un campus, perteneciente a una misma organización. Empiezan por **fec0:.**

- Global, para identificar interfaces en toda Internet. Éstas comienzan por **2001:** ó **3ffe:.**

En lo que a ámbito se refiere, las direcciones anycast siguen la misma norma que las unicast.

Sin embargo, para las direcciones multicast tenemos catorce posibles ámbitos, que identifican desde una interfaz local a una dirección global.

Nodos de un mismo ámbito y visibles entre sí definen una zona. No se permite que un router encamine tráfico entre diferentes zonas (perderían todo el sentido los ámbitos).

Una de las grandes ventajas de los ámbitos es que permitiría la renumeración de prefijos sin mucha dificultad, ya que las direcciones de ámbito no global se mantendrían. Se debe esperar a que se produzca alguna renumeración de prefijos globales, ya que según crezca una organización su prefijo se puede quedar pequeño y necesitar más espacio de direcciones. Y como se ha dicho antes, se trataría siempre que sea posible de mantener las tablas de encaminamiento al mínimo. Lo que sólo se consigue dando un prefijo nuevo mayor e invalidando el anterior, porque lo que seguramente sucedería sería que las redes contiguas ya estén asignadas.

## 3.3. NOMENCLATURA DE LAS DIRECCIONES.

Se tienen tres formas comunes de representar direcciones IPv6 en texto:

- x:x:x:x:x:x:x:x, donde cada x es el valor en hexadecimal de cada grupo de 16 bits de la dirección.

- x:x::x, en el caso de que haya grupos contiguos de 16 bits todos cero. Es una abreviatura que serviría para hacer más "cómodo" el uso de algunas direcciones.

- x:x:x:x:x:x:d.d.d.d, donde las x son los seis grupos de 16 bits en hexadecimal de mayor peso de la dirección y las d son los valores decimales de los cuatro grupos de 8 bits de menor peso de la dirección. Esta forma es a veces más conveniente a la hora de manejar entornos mixtos IPv6 e IPv4. Por ejemplo: 0:0:0:0:0:FFFF:129.144.52.38 y en su forma abreviada ::FFFF:129.144.52.38.

| Representación Normal | Representación Abreviada | Tipo |
|---|---|---|
| 1080:0:0:0:8:800:200C:417A | 1080::8:800:200C:417ª | Unicast |
| FF01:0:0:0:0:0:0:101 | FF01::101 | Multicast |
| 0:0:0:0:0:0:0:1 | ::1 | Loopback |
| 0:0:0:0:0:0:0:0 | :: | No Especificada |

**Tabla 3-1. Nomenclatura de direcciones IPv6**

## 3.4. NOMENCLATURA DE LOS PREFIJOS.

La representación de los prefijos de direcciones con IPv6 es similar a la que tenemos con CIDR con IPv4, esto es: dirección-IPv6/tamaño-prefijo.

Donde dirección-IPv6 es alguna de las notaciones vistas en la sección anterior y tamaño-prefijo es un valor decimal que especifica cuantos bits de la dirección corresponden al prefijo. Por ejemplo, el prefijo de la UJI en hexadecimal es 3FFE33300002, que son 48 bits, lo podemos escribir como:

- ✓ 3FFE:3330:0002:0000:0000:0000:0000:0000/48
- ✓ 3FFE:3330:2:0:0:0:0:0/48
- ✓ 3FFE:3330:2::/48

Si se quiere escribir la dirección y el prefijo, no hace falta que se escriba los dos de forma explícita. Por ejemplo, una dirección IPv6 de la misma UJI con su prefijo asociado quedará 3FFE:3330:2:1:250:BAFF:FE7A:E67E/48.

## 3.5. REPRESENTACIÓN DE DIRECCIONES.

Las direcciones IPv4 son típicamente representadas en notación con punto decimal. Así, una dirección de 32 bits es dividida en 4 direcciones de 8 bits, y cada sección es representada por un número decimal entre 0 y 255:

128.138.213.13.

Como las direcciones IPv6 son de 128 bits de longitud, un método diferente de representación es requerido. Como se especificó en RFC 2373, la representación preferida es: x:x:x:x:x:x:x:x donde x representa 16 bits, y cada una de esas secciones de 16 bits es definida en hexadecimal. Por ejemplo: una dirección IPv6 podría ser de la forma:

FEDC:BA98:7654:3210:FEDC:BA98:7654:3210.

Nótese que cada una de las secciones de 16 bits es separada por ":", y que cada 4 números hexadecimales son usados para representar cada sección de 16 bits. Si alguna sección contiene ceros al principio, esos ceros no son requeridos. Por ejemplo: 1080:0000:0000:0000:0008:0800:200C:417A puede ser simplificada a: 1080:0:0:0:8:800:200C:417A. Si aparecen largas cadenas de ceros en una dirección, "::" puede ser usado para indicar múltiples grupos de 16 bits de ceros, que luego simplifican la dirección de arriba a: 1080::8:800:200C:417A.

El uso de "::" es restringido a aparecer solo una vez en una dirección, aunque puede ser usado para comprimir o los ceros del principio o los subsiguientes en una dirección. Por ejemplo, una dirección 'loopback' de: 0:0:0:0:0:0:0:1 podría ser simplificada a: ::1.

Cuando las direcciones IPv6 son expresadas en texto, es común delinearlas como dirección y longitud de prefijo: IPv6-address/prefix-length donde la dirección IPv6 es expresada en una de las notaciones listadas anteriormente, y la longitud de prefijo es un valor decimal que especifica el número de los bits más a la izquierda de la dirección comprimida en el prefijo. Por ejemplo:

12AB:0000:0000:CD30:0000:0000:0000:0000/60 indica que el prefijo de 60 bits (en hexadecimal) es: 12AB00000000CD3.

### 3.6. ARQUITECTURA.

Las direcciones IPv6 de 128 bits pueden ser divididas en un número de subcampos para proveer máxima flexibilidad para tanto las representaciones actuales como las futuras. Los bits líderes, llamados el Prefijo de Formato (Format Prefix), definen el tipo específico de dirección IPv6. RFC 2373 define un número de esos prefijos.

Nótese que el espacio de dirección ha sido asignado por NSAP, IPX, unicast global, multicast y otros tipos de direcciones. Al tiempo de este escrito, 15% del espacio de dirección ha sido asignado y el 85% restante ha sido reservado para uso futuro.

Una dirección multicast comienza con el valor binario 11111111; cualquier otro prefijo identifica una dirección unicast. Las direcciones anycast son parte de la asignación de las direcciones unicast y no se les da un identificador único.

Nótese que RFC 2373 define 2 contextos adicionales referentes a la arquitectura de direccionamiento de IPv6. Primero, los tipos exclusivos de direcciones especiales son asignados fuera del prefijo de formato 0000 0000. Estas son las direcciones No Especificadas, Loopback y de Compatibilidad que contienen direcciones IPv4 encajado.

Segundo, algunas direcciones IPv6 contienen identificadores acoplados en la interfaz. Los formatos de prefijo 001 hasta 111, esperan por direcciones multicast (prefijo de formato 1111 1111) requieren todos tener identificadores de interfaz de 64 bits especificados en el formato IEEE EUI-64.

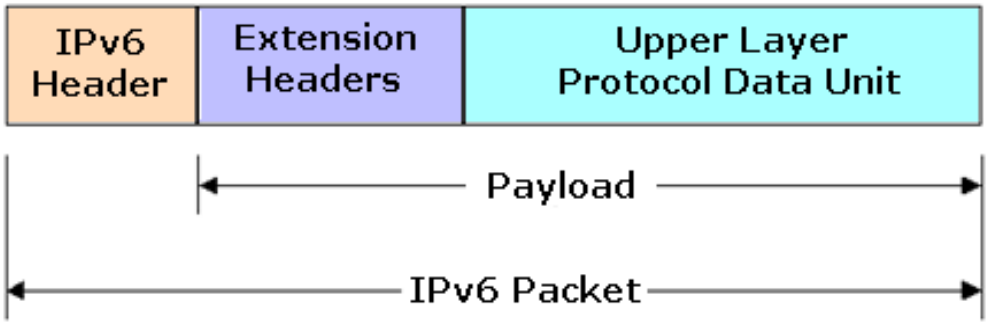



**Fig. 3-4. Arquitectura de una Dirección IPv6.**

| PREFIJO (Binario) | ASIGNACION |
|---|---|
| 0000 0000 | Reservado |
| 0000 0001 | Sin Asignar |
| 0000 0010 | Reservado para asignaciones NSAP |
| 0000 0100 | Reservado para asignaciones IPX |
| 0000 0110 | Sin Asignar |
| 0000 1000 | Sin Asignar |
| 0001 0000 | Sin Asignar |
| 0010 0000 | Aggregatable Global Unicast Addresses |
| 0110 0000 | Sin Asignar |
| 1000 0000 | Sin Asignar |
| 1010 0000 | Sin Asignar |
| 1100 0000 | Sin Asignar |
| 1110 0000 | Sin Asignar |
| 1111 0000 | Sin Asignar |
| 1111 1000 | Sin Asignar |
| 1111 1100 | Sin Asignar |
| 1111 1110 0 | Sin Asignar |
| 1111 1110 10 | Link Local Unicast Addresses |
| 1111 1110 11 | Site Local Unicast Addresses |
| 1111 1111 | Multicast Addresses |

**Tabla 3-2. Identificadores de Interfaz para direccionamiento.**

### 3.6.1. DIRECCIONES UNICAST.

Existen varios tipos de direcciones unicast en IPv6, como las globales agregables, las Site-Local, las Link-Local, las IPX jerárquicas, la NSAP, y las compatibles IPv4. Más tipos de direcciones pueden ser definidos en el futuro.

Dependiendo del papel que realice cada nodo, éste puede tener más o menos conocimiento de la estructura del paquete IPv6. Por ejemplo, un nodo puede considerar una dirección IPv6 unicast como un “todo” siendo inconsciente incluso

de los prefijos; algo más complejo entendería de prefijos y, yendo un poco más lejos, podría entender la jerarquía dentro del prefijo y lo que ello implica.

Un número de formas para direcciones unicast ha sido definido para IPv6, algunas con estructuras más complejas que proveen asignaciones de dirección jerárquica. La forma más simple es una dirección unicast sin estructura interna, en otras palabras, sin jerarquía de dirección definida.

La próxima posibilidad sería especificar un prefijo de subred (Subnet Prefix) dentro de la dirección de 128 bits, así dividir la dirección en un prefijo de subred (con n bits) y un ID de interfase (128 – n bits).

Algunas direcciones especiales son también definidas en RFC 2373.

La dirección 0:0:0:0:0:0:0:0 (también representada 0::0, o simplemente ::) es definida como la dirección no especificada , que indica la ausencia de una dirección. Esta dirección podría ser usada en el inicio cuando un nodo todavía no tiene una dirección asignada. La dirección no especificada puede nunca ser asignada a cualquier nodo.

La dirección 0:0:0:0:0:0:0:1 (también representada 0::1, o simplemente ::1) igual a 127.0.0.1 de IPv4, es definida como la dirección loopback . Esta dirección es usada por un nodo para enviar un paquete a sí mismo. La dirección loopback puede nunca ser usada a cualquier interfaz. Un paquete IPv6 con una dirección destino de la dirección loopback nunca debe ser enviado fuera de un nodo simple, y nunca debe ser reenviado por un router IPv6.

#### 3.6.1.1. Direcciones de compatibilidad

Dos direcciones de transición han sido definidas para las redes de transición IPv4/IPv6.

La primera dirección es llamada una dirección IPv4 compatible con IPv6. Es usada cuando 2 dispositivos IPv6 (como hosts o routers) necesitan comunicarse vía una infraestructura de ruteo IPv4. Los dispositivos en la punta de IPv4 usarían esta dirección unicast especial, que carga una dirección IPv4 en el orden bajo de 32 bits. Este proceso es llamado túneles automático. Nótese que el prefijo es 96 bits de ceros.

El segundo tipo de dirección de transición es llamado IPv4 tras la dirección IPv6. Esta dirección es usada por los nodos de solo IPv4 que no soportan IPv6. Por ejemplo, un host IPv6 usaría IPv4 a través de la dirección IPv6 para comunicarse

con otro host que solo soporte IPv4. Nótese que el prefijo es 80 bits de ceros seguido de 16 bits de unos.

### 3.6.1.2. Direcciones que soportan la arquitectura OSI

Muchas redes incorporan elementos derivados de los protocolos OSI (Open Systems Interconnection) en sus arquitecturas de direccionamiento y ruteo. Un ejemplo OSI es el Protocolo de Redes sin Conexión, ISO 8473, y su esquema de direccionamiento, que usa direcciones NSAP (Network Service Access Point).

Otros ejemplos son los protocolos de ruteo OSI, End System to Intermediate System (ES-IS), definidos en ISO 9542, o el Intermediate System to Intermediate System (IS-IS), definido en ISO 10589. Desde que las direcciones NSAP (llamadas NSAPAs) son típicamente de 20 octetos de longitud, los mecanismos deben ser proveídos para adaptar este formato al de la estructura de direcciones IPv6 de 16 bits. Las direcciones que soportan NSAPAs tienen un prefijo de formato de 7 bits de 0000001.

RFC 1888 define 4 mecanismos para soportar el direccionamiento OSI NSAP en una red IPv6:

- NSAPA restringido mapeando en direcciones IPv6 de 16 octetos.
- NSAPA truncado para ruteo, NSAPA completo en la opción IPv6.
- Dirección IPv6 normal, NSAPA completo en la opción IPv6.
- Direcciones IPv6 cargadas como direcciones OSI

Cuando las NSAPA son mapeadas en direcciones IPv6 de 16 octetos, un bit cero continúa el prefijo de formato 0000001, rendimiento de un primer octeto de 00000010. Los campos subsecuentes incluyen un código del formato de la autoridad (AFcode), cuál codifica el identificador de la autoridad y del formato (AFI), un indicador inicial del dominio (IDI), un prefijo, un área, y un End System ID.

Una NSAPA truncada utilizada como una dirección IPv6 toma los octetos de orden alto de la dirección NSAP, que incluye la información de ruta que consiste de Routing Domain y los identificadores de Área, y entonces trunca otros campos NSAP que no son requeridos.

Una tercera alternativa es cargar NSAPAs completas como una opción dentro del encabezado Destination Options. Nótese que Option Type = 195 (decimal) y que las NSAPAs completas (20 octetos) son entonces incluidas en el encabezado Destination Option.

La alternativa final permite a una dirección IPv6 ser fijada dentro de una dirección NSAP de 20 octetos. El primer octeto es un Authority and Format Indicator, y los dos octetos próximos son conocidos como Internet Code Point (ICP). Tomados juntos, estos 3 octetos comprenden el Initial Domain Part (IDP) de la NSAPA. Los próximos 16 octetos contienen la dirección IPv6; el octeto final, llamado un selector, está configurado en cero.

### 3.6.1.3. Direcciones IPX

Las direcciones IPX (Internetwork Packet Exchange) deberían ser mapeados en direcciones IPv6 con un formato que comienza con el formato de prefijo de 7 bits 0000010. El balance de esta dirección todavía está bajo estudio.

### 3.6.1.4. Direcciones unicast globales agregables.

Muchas redes de comunicaciones, como la red de teléfonos global, son basadas en un esquema de direccionamiento jerárquico. Una jerarquía facilita un escalamiento y ruta más fáciles. Por ejemplo, llamadas dentro de Norteamérica requieren el Código de Zona de Norteamérica (1), el Código de Área (Ejemplo 303), el Código de Oficina Central (Ejemplo 555), y el Número de Línea (1212).

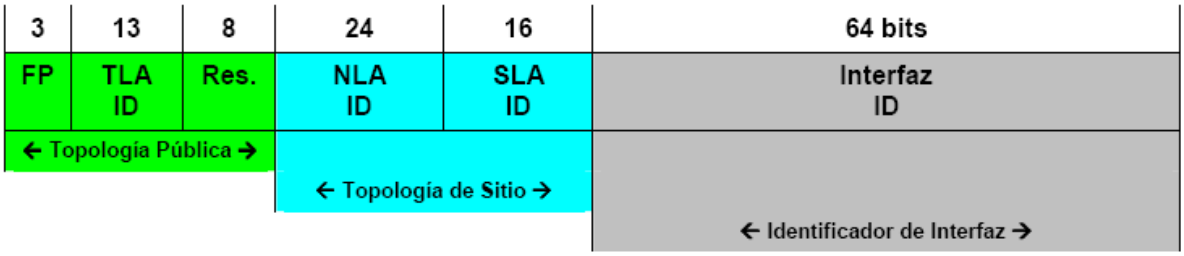
Llamadas desde Norteamérica a Londres requieren el Código de Acceso Internacional (011), el Código de País (44 para el Reino Unido), un Código de Ciudad (71 para Londres), y entonces el número de teléfono local. Si la red crece, podría agregar otro Código de Área o de País, que facilita el desafío de escalamiento. Si va a llamar a dentro del país, no hay necesidad de marcar el Código de Acceso Internacional o el Código de País, que facilita el desafío de ruta.

Para IPv6, la jerarquía para las direcciones agregables es organizada en 3 niveles: una topología pública, una topología de sitio y un identificador de interfase, como se documenta en RFC 2374. La topología pública es la colección de proveedores e intercambios que provee el servicio de tránsito del Internet público. La topología de site es local a un site u organización específica, pero no provee servicio de tránsito público a nodos fuera de su site. Los identificadores de interfase proveen identificación única para interfases en un link específico.

(Como una nota histórica, el formato de la Dirección Agregable Unicast Globales reemplazó el previamente definido formato Dirección Unicast Basado en el Proveedor, que fue definido en RFC 2073. El formato Agregable mejora el formato Basado en el Proveedor en un número de formas. RFC 2073 es ahora considerado como 'histórico'.)

Así, una arquitectura basada en adición incluiría los proveedores mundiales, los intercambios y suscriptores. Los intercambios asignarán direcciones IPv6. En algunos casos, los suscriptores se conectarían directamente a un intercambio. Esto proveería acceso a múltiples proveedores intercontinentales y permitirán un cambio de proveedores sin tener que reenumerar su organización.

La dirección agregable unicast global comienza con un formato de prefijo de 001 e incluye otros 4 campos que especifican varios niveles de jerarquía. El identificador de Agregación de Alto Nivel (TLA – Top-Level Aggregation Identifier) es un campo de 13 bits. Así, 8,192 (213) TLAs pueden ser asignados por cada valor de formato de prefijo definido. Una propuesta para la asignación de TLAs está documentada en RFC 2450.




Donde:

| | |
|---|---|
| **FP** | Prefijo de Formato (001) - Format Prefix |
| **TLA ID** | Identificador de Agregación de Nivel Superior - Top-Level Aggregation Identifier |
| **Res.** | Reservado para uso futuro |
| **NLA ID** | Identificador de Agregación de Siguiente Nivel - Next-Level Aggregation Identifier |
| **SLA ID** | Identificador de Agregación de Nivel de Sitio - Site-Level Aggregation Identifier |
| **Interfaz ID** | Identificador de Interfaz |

**Fig. 3-5. Dirección Agregable Unicast Local.**

El campo Reserved (Res.), que tiene 8 bits de longitud, está proveído para permitir la expansión más amplia de campos TLA o NLA como la experiencia adicional con IPv6 es cumplida.

Cada organización a la que un TLA es asignado es proveída con 24 bits de espacio de dirección Next-Level Aggregation Identifier (NLA ID). El espacio NLA ID es entonces usado por las organizaciones para crear una jerarquía de direccionamiento y para identificar sites. El uso de NLA está también propuesto en RFC 2450.

El espacio de 24 bits NLA ID puede ser asignado en varios niveles de sites. La organización responsable de TLA define el diseño de BIT del espacio NLA. El diseño de BIT del siguiente nivel NLA es la responsable del nivel previo NLA ID (como NLA1), NLA ID constituye la Topología Pública (64 bits totales).

El identificador de Agregación del Nivel de Site (SLA ID – Site-Level Aggregation Identifier) es un campo de 16 bits que permite a organizaciones individuales crear una jerarquía de direccionamiento local. El campo SLA ID puede soportar 65,535 (216) subredes individuales. Jerarquías múltiples de subredes pueden ser también definidas.

| n | 24-n bits | | 16 | 64 bits |
|---|---|---|---|---|
| NLA1 | Site ID | | SLA ID | Interfaz ID |
| | m | 24-n-m bits | 16 | 64 bits |
| | NLA2 | Site ID | SLA ID | Interfaz ID |
| | | o 24-n-m-o bits | 16 | 64 bits |
| | | NLA3 Site ID | SLA ID | Interfaz ID |

**Fig. 3-6. Identificador de Agregación de Siguiente Nivel.**

| n | 16-n bits | | 64 bits |
|---|---|---|---|
| SLA1 | Subred | | Interfaz ID |
| | m | 16-n-m bits | 64 bits |
| | SLA2 | Subred | Interfaz ID |

**Fig. 3-7. Identificador de Agregación de Nivel de Sitio.**

El último campo es el identificador de Interfase (Interface Identifier), que identifica las interfases en un enlace. Cada ID de Interfase tiene 64 bits de longitud y es estructurado de acuerdo al formato IEEE EUI-64, que será discutido en una sección siguiente.

### 3.6.1.5. Identificadores de interfaz

Los identificadores de interfaz en las direcciones unicast IPv6 se utilizan para identificar interfaces en un determinado enlace (una LAN, por ejemplo). Es necesario que sean únicos en el enlace, porque si se dejan de identificar interfaces al nivel de enlace ya no hay nada más que hacer. Pero esto último no significa que puedan seguir siendo únicos en un ámbito mayor que el de enlace.
Por norma general, los identificadores se obtendrán a partir de las direcciones de la capa de enlace.

Unos cuantos tipos de prefijos requieren identificadores de interfaz de 64 bits y, además, estar construidos en formato IEEE EUI-64. Estos identificadores pueden ser globales en el caso de que un token global esté disponible, como los 48 bits del MAC, o locales en caso de que no lo esté, como un enlace por puerto paralelo o los extremos de un túnel.

Se requiere que el bit 'u' sea invertido en caso de que el identificador se haya construido a partir del formato EUI-64. Este bit, según la terminología IEEE es el que indica la localidad o universalidad del identificador. Esto, que en un principio no tiene mucho sentido, va a servir para que aquellas interfaces donde no es posible obtener un token global tengan una forma más sencilla. Por ejemplo, un extremo de un túnel, su identificador debería ser 0200:0:0:1 en vez de ::1 si este cambio no fuera posible.

### 3.6.1.6. Direcciones IPv6 con Direcciones IPv4.

Dentro de los mecanismos previstos de transición de IPv4 a IPv6, existe una técnica que permite a los hosts y routers entunelar dinámicamente paquetes IPv6 sobre la infraestructura IPv4 existente. Los nodos que vayan a utilizar esta técnica recibirán una dirección IPv4. A este tipo de direcciones se les llama direcciones IPv6 compatibles con IPv4.

También existe otro tipo de dirección IPv6 que contiene a una IPv4 y se utilizará para representar aquellos nodos que sólo disponen de pila IPv4 En este caso los 32 bits más bajos serán iguales que en el caso anterior (la dirección IPv4), pero

los 16 bits siguientes por delante serán todos 1. Este tipo de direcciones recibe el nombre de direcciones IPv6 mapeadas IPv4.

### 3.6.2. DIRECCIONES DE PRUEBA.

Una asignación especial ha sido propuesta para el propósito de probar software IPv6 y es descrita en RFC 2471. (Esta asignación de direcciones de prueba tiene como intención reemplazar la asignación de prueba anterior definida en RFC 1897.) Estas direcciones son solo para ser usadas para prueba de IPv6 y no son ruteables en el Internet. El formato de las direcciones de prueba está basado en la Dirección Unicast Global Agregable, con sus varios campos asignados como sigue:

**FP: 001** (Asignado a la Dirección Unicast Global Agregable).
**TLA ID: 1FFE H** (Asignado para prueba 6bone).
**NLA ID** (Asignado por el administrador TLA).
**SLA ID** (Asignado por la organización individual).
**Interface ID:** Un identificador de interfase para ese link (Ethernet, token ring, etc.)

Nótese en la figura 3-8, que el formato de las Direcciones de Prueba no contiene el campo Reserved, que estaba incluido entre los campos TLA y SLA en la Dirección Unicast Global Agregable para permitir futura expansión de cualquier espacio de dirección. El formato de las Direcciones de Prueba define una función específica de direccionamiento, y sus desarrolladores eligieron asignar los bits de Reserved a NLA ID, haciendo que el campo NLA tuviera 32 bits de longitud.

### 3.6.3. DIRECCIONES DE USO LOCAL

Dos direcciones están definidas para uso local solamente. La dirección Link- local es usada por un link simple y su intención es la configuración de auto dirección, descubrimiento de vecino (Neighbor Discovery), o cuando no hay routers presentes. La dirección Link-local comienza con el Formato de Prefijo 111111101 e incluye un campo Inteface ID de 64 bits. Los routers nunca reenvían paquetes con la dirección destino o fuente Link -local hacia otros links (enlaces).

La dirección Site-local es usada por las organizaciones que todavía no se han conectado al Internet. En vez de fabricar una dirección IPv6, ellos pueden usar la dirección Site-local. Los routers nunca reenvían paquetes con las direcciones fuente Site-local fuera de ese site. Esta dirección comienza con el Formato de Prefijo 1111111011 e incluye tanto un campo Subnet ID de 16 bits como un campo Interface ID de 64 bits.

### 3.6.4. DIRECCIONES ANYCAST

Una dirección anycast es aquella que es asignada a múltiples interfases, típicamente en nodos diferentes. Un paquete con una dirección destino anycast es ruteado a la interfase más cercano teniendo esta dirección, como se midió en la definición de distancia del protocolo de ruteo. El concepto de hacer anycast dentro de trabajos de Internet basado en IP fue propuesto por primera vez en RFC 1546.

RFC 2373 nota varios usos posibles para la dirección anycast:

1. Identificar un set de routers pertenecientes a un ISP
2. Identificar el set de routers pegado (attached) a una subred particular.
3. Identificar el set de routers que proveen entrada a un dominio de ruteo particular.

Dos restricciones son puestas en las direcciones anycast. Primero, ellas no deben ser usadas como direcciones fuente para un paquete IPv6. Segundo, una dirección anycast puede solo ser asignada a routers, no a hosts.

Una dirección anycast es predefinida y requerida: la dirección anycast Subnet-Router. Esta dirección comienza con un prefijo de subred de longitud variable y concluye con ceros para rellenar. Todos los routers en esa subred deben soportar esta dirección anycast. Su intención es ser usada en aplicaciones donde un nodo necesita comunicarse con un miembro de un grupo de routers en una subred remota.

Trabajo adicional ha sido propuesto que define un set de direcciones anycast reservadas dentro de cada prefijo de subred. Asignaciones de direcciones anycast adicionales esperan a ser definidas en el futuro.

| n Bits | 128-n Bits |
|---|---|
| **Prefijos de Subred** | **0000000000000000000** |

**Fig. 3-8. Formato de Dirección Anycast.**

### 3.6.5. DIRECCIONES MULTICAST.

La dirección multicast identifica un grupo de nodos, y cada uno de estos nodos puede pertenecer a múltiples grupos multicast. Las direcciones multicast son definidas en RFC 2373 y documentadas en más detalle en RFC 2375.

La dirección multicast comienza con el Formato de Prefijo 11111111 e incluye 3 campos adicionales. El campo Flags contiene cuatro flags (banderas) de 1 BIT. Los 3 bits de las banderas más significantes están reservados para uso futuro y son inicializados en cero. La cuarta bandera es llamada el BIT T, o transitorio. Cuando T=0, la dirección multicast es una dirección multicast permanentemente asignada (o mejor conocida), asignada por la autoridad de numeración de Internet global. Cuando T=1, un transitorio (o asignación no permanentemente) de dirección multicast es indicada.

| 8 | 4 | 4 | 112 Bits |
|---|---|---|---|
| 11111111 | 000T | Ámbito | Identificador de Grupo |

**Fig. 3-9. Formato de Dirección Multicast.**

El campo Scop (Ámbito) es un campo de 4 bits que es usado para limitar el alcance del grupo multicast. Los valores del campo Scop se presentan en la tabla 3-3:

| VALOR | SIGNIFICADO |
|---|---|
| **0** | Reservado |
| **1** | Alcance de Nodo Local |
| **2** | Alcance de Link Local |
| **3** | Sin Asignar |
| **4** | Sin Amigar |
| **5** | Alcance de Site Local |

| | |
|---|---|
| **6** | Sin Asignar |
| **7** | Sin Asignar |
| **8** | Alcance de Organización Local |
| **9** | Sin Asignar |
| **A** | Sin Asignar |
| **B** | Sin Asignar |
| **C** | Sin Asignar |
| **D** | Sin Asignar |
| **E** | Alcance Global |
| **F** | Reservado |

**Tabla 3-3. Valores del Campo Scop.**

El campo Group ID identifica el grupo multicast, sea permanente o transitorio, dentro del alcance dado. Las direcciones multicast no pueden ser usadas como direcciones fuente en los datagramas IPv6 o aparecer en ningún encabezado de encaminamiento. RFC 2373 documenta las siguientes direcciones multicast predefinidas:

**DIRECCIONES MULTICAST RESERVADAS:**

FF00:0:0:0:0:0:0:0
FF01:0:0:0:0:0:0:0
FF02:0:0:0:0:0:0:0
FF03:0:0:0:0:0:0:0
FF04:0:0:0:0:0:0:0
FF05:0:0:0:0:0:0:0
FF06:0:0:0:0:0:0:0
FF07:0:0:0:0:0:0:0
FF08:0:0:0:0:0:0:0
FF09:0:0:0:0:0:0:0
FF0A:0:0:0:0:0:0:0
FF0B:0:0:0:0:0:0:0
FF0C:0:0:0:0:0:0:0

FF0D:0:0:0:0:0:0:0
FF03:0:0:0:0:0:0:0
FF0F:0:0:0:0:0:0:0

Las direcciones multicast están reservadas y nunca serán asignadas a ningún grupo multicast.

**TODAS LAS DIRECCIONES DE LOS NODOS:**

FF01:0:0:0:0:0:0:1
FF02:0:0:0:0:0:0:1

Las direcciones multicast identifican el grupo de todos los nodos IPv6 dentro del alcance 1 (nodo local) o 2 (link local). Por ejemplo, la dirección FF02:0:0:0:0:0:0:1 (o FF02::1) tiene el significado 'todos los nodos en este link'.

**TODAS LAS DIRECCIONES DE LOS ROUTERS:**

FF01:0:0:0:0:0:0:2
FF02:0:0:0:0:0:0:2
FF05:0:0:0:0:0:0:2

Las direcciones multicast identifican el grupo de todos los routers IPv6 dentro del alcance 1 (nodo local), 2 (link local) o 5 (site local). Por ejemplo, la dirección FF02:0:0:0:0:0:0:2 (o FF02::2) tiene el significado 'todos los routers en este link'.

**DIRECCIONES DE NODO SOLICITADO:**

FF02:0:0:0:0:1:FFXX:XXXX

La dirección multicast es computada como una función de direcciones unicast y anycast. La dirección multicast de nodo solicitado está formada tomando los 24 bits de orden bajo de la dirección (unicast o anycast) y agregando esos bits al prefijo de 104 bits FF02:0:0:0:0:1:FF00::/104.

Esto resulta en una dirección multicast en el rango:
FF02:0:0:0:0:1:FF00:0000 hasta FF02:0:0:0:0:1:FFFF:FFFF.
Por ejemplo, la dirección multicast de nodo solicitado correspondiente a la dirección IPv6 4037::01:800:200E:8C6C es FF02::1:FF0E:8C6C.

Las direcciones IPv6 que solo difieren en los bits de alto orden, por ejemplo, debido a múltiples prefijos de orden alto asociados con diferentes agregaciones (proveedores), se mapearán a la misma dirección de nodo solicitado. Esto reduce el número de direcciones multicast que un nodo debe conectar (juntar). Un nodo es requerido para computar y suportar a una dirección multicast de nodo solicitado por cada dirección unicast y anycast que son asignadas.

## 3.7. CALIDAD DE SERVICIO (QUALITY OF SERVICES – QoS)

Los campos de la etiqueta de la prioridad y del flujo en el encabezado IPv6 son utilizados por una fuente para identificar los paquetes que necesitan la dirección especial por los routers de la red. El concepto de un flujo en el IP es una salida importante de IPv4 y de la mayoría de los otros protocolos sin conexión; algunos han llamado flujos que una forma de circuitos virtuales sin conexión desde todos los paquetes con la misma etiqueta del flujo se trata semejantemente y la red lo visualiza como entidades asociadas.

La dirección especial para quality-of-service que no están por defecto, es los usos de una ayuda importantes de la capacidad para que requieran rendimiento de procesamiento garantizado, end-to-end retrasado, e inquietud, por ejemplo multimedia o comunicación en tiempo real.

El campo de prioridad permite que la fuente identifique la prioridad deseada de un paquete. Los valores 0-7 se utilizan para controlar el tráfico congestionado, o el tráfico que retrocede en respuesta a la congestión de red, tal como segmentos del TCP. Para este tipo de tráfico, se recomiendan los valores siguientes de la prioridad:

1. Tráfico sin Caracterizar.
2. Tráfico “relleno”.
3. Transferencia de datos desatendida. (Ejemplo: E-mail)
4. Reservado
5. Transferencia a Granel Atendida. (Ejemplo: FTP, HTTP, NFS)
6. Reservado
7. Tráfico Interactivo. (Ejemplo: Telnet, SSH, X)
8. Tráfico del control del Internet (Ejemplo: SNMP)

Los valores 8-15 se definen para controlar el tráfico de no-congestión, o el tráfico que no retrocede en respuesta a la congestión de red, tal como paquetes en tiempo real que son enviados en una tarifa constante. Para este tipo de tráfico, el valor más bajo de la prioridad (8) se debe utilizar para los paquetes que el

remitente está el más dispuesto a haber desechado bajo condiciones de la congestión (Ejemplo: tráfico video de alta fidelidad) y el valor más alto (15) se debe utilizar para esos paquetes que el remitente está lo más menos posible dispuesto a haber desechado (Ejemplo: Voz sobre IP).

La etiqueta del flujo es utilizada por una fuente para identificar los paquetes que necesitan el QoS; no están por defecto. La naturaleza de la dirección especial se pudo transportar a los routers de la red por un protocolo del control, tal como el protocolo de la reservación del recurso (RSVP), o por la información dentro de los paquetes del flujo ellos mismos, tales como una opción del salto- por-salto. Puede haber flujos activos múltiples de una fuente a una destinación, así como el tráfico que no se asocia a ningún flujo (es decir, etiqueta del flujo = 0). Un flujo es identificado únicamente por la combinación de una dirección de la fuente y de una etiqueta distinta a cero del flujo. Este aspecto de IPv6 todavía está en la etapa experimental y la definición del futuro espera.

Las figuras 3-10 y 3-11 muestran la función QoS y su esquema, respectivamente:

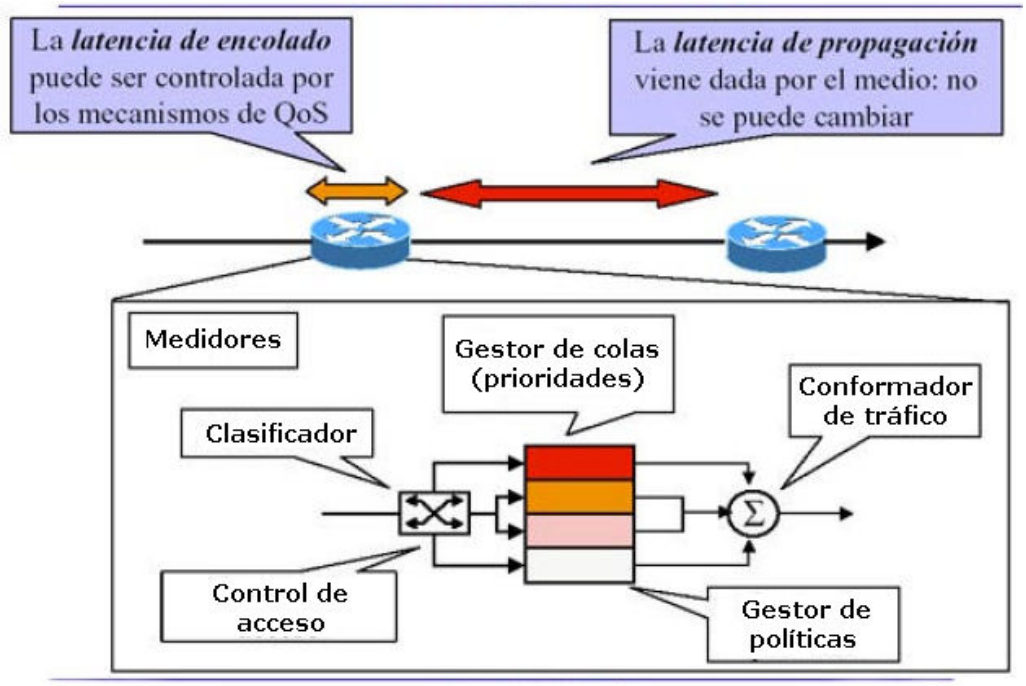



**Fig. 3-10. QoS.**

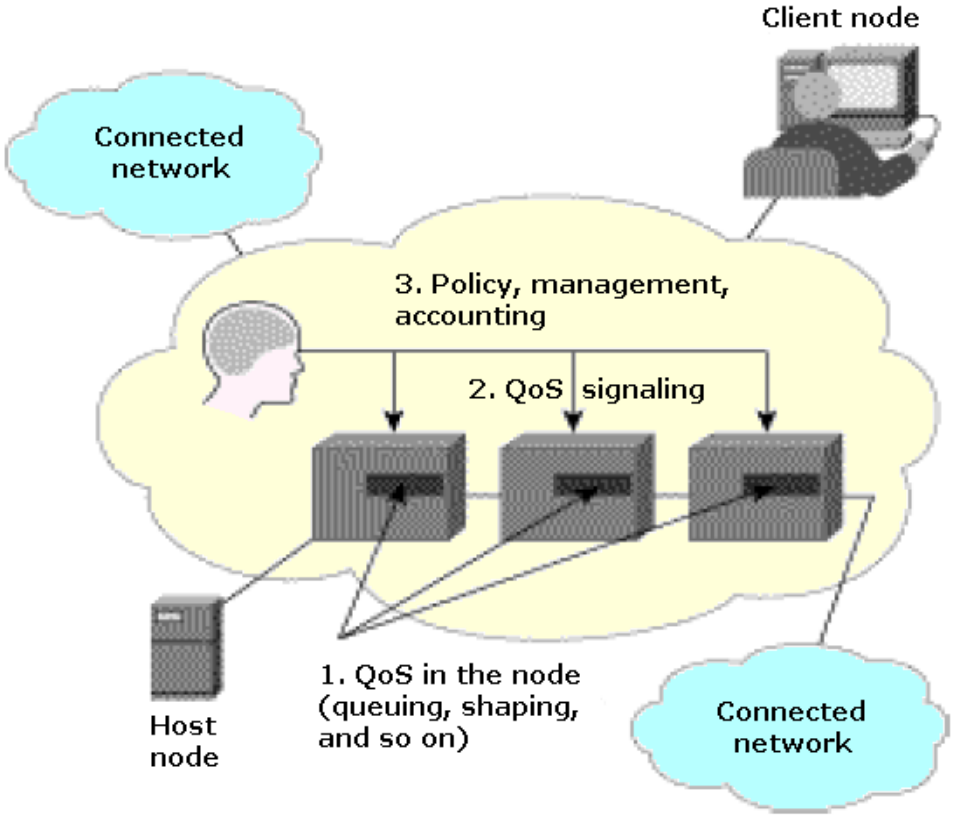



**Fig. 3-11. Esquema de QoS.**

### 3.8. REQUERIMIENTO DE NODO.

El RFC 2373 resume los siguientes requerimientos paras los nodos y sus direcciones:

De un host es requerido que reconozca las siguientes direcciones mientras se identifican a si mismo:

- Su dirección de enlace local (Link -Local) para cada interfaz.
- Su dirección unicast asignada.
- Su dirección de loopback.
- Su dirección multicast de “todos los nodos”.

- La dirección multicast de todos los grupos a los que pertenezca.

Además, si el nodo es un router, se requiere que reconozca también:

- Las direcciones anycast de cada subred para la que es router.
- Las direcciones anycast que se le han asignado.
- La dirección multicast de “todos los routers”.

Los únicos prefijos de direcciones que deben ser predefinidos en una implementación son los siguientes:

- La dirección no específica.
- La dirección de loopback.
- El prefijo multicast (FF).
- Los prefijos locales de enlace y de ‘sitio’ (link-local y site-local).
- Las direcciones multicast predefinidas.
- Los prefijos compatibles IPv4.

Las implementaciones deben asumir que todas las otras direcciones son unicast al menos que este específicamente configurado (Ejemplo, direcciones anycast).

# CAPITULO IV

# CAPITULO IV: AUTO CONFIGURACIÓN Y RED LOCAL

## 4.1. OBJETIVO DEL DISEÑO.

Como hemos visto hasta ahora, IPv6 tiene algunas capacidades (y algunas complejidades) que van más allá de lo que IPv4 ofrece en el presente.

Afortunadamente, los arquitectos de IPv6 desarrollaron protocolos y procesos adicionales que mejoran esas complejidades.

En este capítulo, estudiaremos uno de los protocolos más importantes, Stateless Address Autoconfiguration, que permite a una workstation entrar a una red IPv6 al inicio automáticamente. El proceso de auto configuración es también muy útil para administradores de red que están emigrando de sus redes IPv4 existentes a IPv6, pues elimina muchos de los requerimientos para configuración humana de direcciones, parámetros de ruteo, y así. Si el proceso de auto configuración falla, o es inadecuado para una situación particular, el DHCP para IPv6 (DHCPv6) también ha sido definido. Además, hay temas únicos para topologías de LAN o WAN particulares que tienen como factor el tema de implementación.

## 4.2. STATELESS ADDRESS AUTOCONFIGURATION

La palabra auto configuración se describe mejor por sus 2 raíces: auto, que significa “mismo”, y configuración, que significa ”arreglo funcional”. De acuerdo a RFC 2462, el proceso de auto configuración incluye crear direcciones de link- local y verificar su unicidad en el link, así como determinar qué información debe ser auto configurada (direcciones, otra información, o ambas). Nótese que el proceso de auto configuración especificada en RFC 2462 se aplica solo a los hosts; es asumido que los routers están configurados de alguna otra manera.

Hay 3 métodos para obtener direcciones: un mecanismo sin estado, un mecanismo con estado, o ambos. Tanto la auto configuración sin estado como con estado pueden ser usadas simultáneamente. El tipo de auto configuración que está en uso es especificado por el mensaje Router Advertisement.

En un modelo de auto configuración con estado, los hosts obtienen direcciones, información de configuración, parámetros, y así, desde un servidor.

Ese servidor mantiene una base de datos conteniendo la información necesaria y guarda control firme sobre las asignaciones de dirección. El modelo de auto

configuración con estado para IPv6 es definido por el protocolo DHCP para IPv6 (DHCPv6), que se considerará en la sección 4.3.

En contraste, auto configuración sin estado no requiere manual configuración de los hosts, mínima (o ninguna) configuración de routers, y ningún servidor adicional. El acercamiento sin estado es usado cuando un site no se concierne acerca de las direcciones específicas que son usadas, mientras ellas sean únicas y ruteables.

Con la auto configuración sin estado, un host genera su propia dirección usando 2 elementos de información: Información disponible localmente (por ejemplo: disponible desde el host mismo) más información publicitada por routers. La parte del host es llamada un identificador de interfase, que identifica una interfase en una subred. La parte del router viene de un prefijo de dirección que identifica la subred asociada con un link. La dirección derivada es una combinación de estos 2 elementos. Si un router no existe en un survey, el host todavía puede generar un tipo especial de dirección llamada la dirección Link- local. La dirección Link-local puede ser usada solo para comunicación entre nodos unidos al mismo link.

Nótese que el proceso de auto configuración sin estado, como se define en RFC 2462, se aplica solo a los hosts, no a los routers. (Porque los hosts obtienen alguna información de sus direcciones de los routers, estos routers deben ser configurados usando algún otro medio.) La sola excepción de esta regla es que los routers pueden generar sus propias direcciones link-local, y pueden verificar la unicidad de estas direcciones en el link, cuando son boteadas o reiniciadas.

Las direcciones IPv6 son “arrendadas” a una interfase por un particular periodo de tiempo, que puede ser indefinido. Asociado con la dirección es un tiempo de vida indicando que tan largo puede ser limitado a esa interfase. Con la expiración del tiempo de vida, tanto el atascamiento como la dirección se vuelven inválidas, y la dirección puede ser reasignada a otra interfase en el Internet. Para soporte de estos atascamientos, la dirección asignada puede tener 2 fases: preferida, que significa que el uso de esta dirección es sin restricciones; y desaprobada, indicando que el uso adicional de esa dirección es desalentado, en anticipación de un atascamiento inválido.

El proceso de auto configuración sin estado comienza con la generación de una dirección link-local para esa interfase:

La dirección de link -local es generada combinando el prefijo de dirección link-local (1111 1110 10) con un identificador de interfase de 64 bits. El identificador de interfase es específico para una topología LAN o WAN en uso. En muchos casos, es derivado de la dirección del hardware que reside en el ROM en la tarjeta de

interfase de red. Nosotros miraremos los varios identificadores de interfase en las secciones subsecuentes de este capítulo.

(Como nota histórica, los documentos anteriores de IPv6 RFC e Internet Draft usaron el término “token de interfase” en vez del término usado actualmente “identificador de interfase”.)

El próximo paso determina la unicidad de la dirección tentativa que ha sido derivada de combinar el prefijo de link -local y el identificador de interfase. En este paso, un mensaje Neighbor Solicitation es transmitido con la dirección tentativa como la dirección target. Si otro nodo está usando esta dirección, un mensaje Neighbor Advertisement se retorna. En este evento, la auto configuración se detiene requiriendo la intervención manual. Si ninguna respuesta Neighbor Advertisement es retornada, la dirección tentativa es considerada única y la conectividad al nivel de IP con los nodos vecinos es ahora posible. Nótese que tanto los hosts como los routers pueden generar direcciones Link -local usando esta parte del proceso de auto configuración.

La próxima fase es ejecutada solo por los hosts; ésta envuelve escuchar los mensajes Router Advertisement que los routers transmiten periódicamente, o forzar un mensaje Router Advertisement inmediato mediante la transmisión de un mensaje Router Solicitation. Si ningún mensaje Router Advertisements es recibido, significando que no hay routers presentes, un método con estado, como DHCPv6, debe ser usado para completar el proceso de configuración.

Si los routers están presentes, los mensajes Router Advertisement serán periódicamente enviados. De acuerdo con RFC 2461, Router Advertisement incluye 2 flags claves, M y O, que son usadas en el proceso de auto configuración:

- El flag Managed Address Configuration (M) es indicado cuando M = 1. En este caso, los hosts deben usar el protocolo (con estado) administrado para auto configuración de direcciones, además de alguna otra dirección autoconfigurada usando auto configuración de dirección sin estado.

- El flag Other Stateful Configuration (O) es indicado cuando O = 1. Los hosts deben usar el protocolo (con estado) administrado para la auto configuración de otra información (no dirección).

Los mensajes Router Advertisement también pueden incluir una o más de las siguientes opciones: Source Link Layer Address, Maximum Transmission Unit

(MTU), y Prefix Information. De acuerdo con RFC 2461, la opción Prefix Information incluye 2 flags clave, L y A, que pueden ser usadas con auto configuración de dirección:

- El flag On-Link (L) es indicado cuando L = 1, significando que este prefijo puede ser usado para determinación “on-link”.

- El flag Autonomous Address Configuration (A) es indicado cuando A = 1, significando que este prefijo puede ser usado para configuración de direcciones autónomas.

## 4.3. DYNAMIC HOST CONFIGURATION PROTOCOL (DHCPv6)

En algunos casos, como cuando una dirección duplicada existe o routers que no están presentes, un proceso de auto configuración sin estado debe ser usado.

El protocolo Dynamic Host Configuration Protocol version 6 (DHCPv6) provee estos parámetros de configuración a los nodos de Internet. DHCPv6 consiste de 2 elementos: un protocolo que envía información de configuración específica al nodo desde un servidor DHCPv6 a un cliente y un mecanismo para asignar direcciones de red y otros parámetros a nodos IPv6.

DHCPv6 está construido en un modelo cliente-servidor, que confía en un total de 6 mensajes Request and Reply para la comunicación de estos detalles de parámetros. Algunos tipos de nodos DHCPv6 funcionales están definidos:

- Cliente DHCPv6: un nodo que inicia solicitudes en un link para obtener parámetros de configuración.

- Servidor DHCPv6: un nodo que responde a solicitudes de clientes para proveer parámetros de configuración. El servidor puede o no puede estar en el mismo link que el cliente.

- DHCPv6 Relay: un nodo que actúa como un intermediario para enviar mensajes DHCPv6 entre clientes y servidores, y está en el mismo link que el cliente.

- Agente DHCPv6: un servidor en el mismo link que el cliente o un relevo.

La comunicación entre agentes DHCPv6 usa las siguientes bien conocidas direcciones multicast:

FF02:0:0:0:0:0:1:2 grupo multicast Link -Local All-DHCP-Agents
FF05:0:0:0:0:0:1:3 grupo multicast Site Local All-DHCP-Servers
FF05:0:0:0:0:0:1:4 grupo multicast Site Local All-DHCP-Relays

Todos los mensajes DHCPv6 tienen un formato similar, que comienza con un campo Message Type (Msg-type) indicando la función específica. Los parámetros de configuración, que son llamados extensiones, están incluídos en los mensajes DHCPv6. Las extensiones han sido definidas para especificar una dirección IP, husos horarios, DNS, Directory Agent, Network Time Protocol Server, Network Information Server, parámetros de TCP, Client-Server Authentification, y otros parámetros.

Un mensaje DHCPv6 Solicitado es enviado a un cliente (o relay, en el nombre de un cliente) para obtener una o más direcciones de servidor, y es identificado por Msg-type = 1. Este mensaje incluye un flag C, que solicita designación de los recursos del cliente en el servidor. También incluye las direcciones del cliente y posible relevo.

El mensaje DHCPv6 Advertise son enviado por un agente DHCPv6 para informar a un cliente prospecto acerca de la dirección IP donde los mensajes de la petición pueden ser enviados; es identificado por Msg-type=2. Este mensaje incluye una bandera (flag) S, indicando que una dirección del servidor está presente también en el mensaje.

El mensaje DHCPv6 Request es enviado por un cliente para solicitar parámetros desde un servidor DHCPv6; es identificado por Msg-type=3. Este mensaje incluye un flag S, que indica que la dirección del servidor está presente; un flag C, que puede solicitar el servidor para limpiar todos los recursos y aprietos asociados con el cliente, un Transaction Identifier, y algunas direcciones y extensiones.

El mensaje DHCPv6 Reply es enviado por un servidor en respuesta a todos los mensajes Request o Release que son recibidos; es identificado por Msg- type=4. Este mensaje incluye un flag L, que indica que una dirección Link-Local está presente; un Status, que indica el éxito o la razón del fallo de un intercambio de mensaje; un Transaction ID, y las posibles dirección y extensiones Link -Local del cliente.

El mensaje DHCPv6 Release es enviado desde un cliente al servidor (sin asistencia de un relevo) para solicitar el lanzamiento de las extensiones particulares; es identificado por Msg-type=5. Este mensaje incluye un flag D, que

indica que el servidor debe enviar la respuesta directamente al cliente, un Transaction Identifier y algunas direcciones y extensiones.

El mensaje DHCPv6 Reconfigure es enviado desde un servidor a un cliente (sin asistencia de un relevo) para indicar ciertos parámetros, que son especificados en las extensiones, necesarios a ser solicitados de nuevo por el cliente; es identificado por Msg-type=6. Este mensaje incluye un flag N, que indica que el cliente no debe esperar un DHCP Reply en respuesta de un DHCP Request que envié (al servidor) como resultado de un mensaje DHCP Reconfigure. También incluye un Transaction Identifier, un Server Address y extensiones.

## 4.4. IPV6 SOBRE ETHERNET.

Ethernet, originalmente desarrollado por Digital Equipment Corporation (DEC) – ahora parte de Compaq Computer Corporation – Intel Corporation, y Xeros Corporation, ha sido tradicionalmente popular con los trabajos de red basados en TCP/IP. Soporte para IPv6 sobre redes Ethernet está documentado en RFC 2464.

El marco Ethernet puede cargar tanto como 1,500 octetos de datos en el campo de información; así, diríamos que la unidad máxima de transmisión (MTU) para Ethernet es 1,500 octetos. Este tamaño puede ser reducido por un paquete Router Advertisement especificando un MTU más pequeño, como se detalla en RFC 2461. El campo Ethernet Type (Ethertype) contiene el valor 86DDH para especificar IPv6.

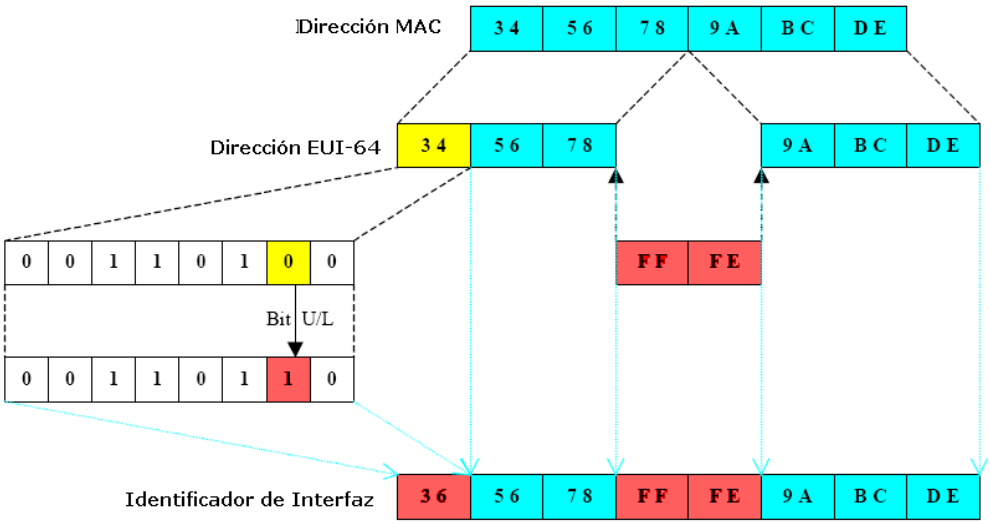



**Fig. 4-1. IPv6 sobre Ethernet.**

La dirección Link-Local es formada preponiendo el prefijo de Link-Local (FE80::0) al identificador de interfase. Para redes Ethernet, el identificador de interfase (interface identifier) es la dirección de Ethernet de 48 bits, expandida en el centro con los caracteres hexadecimales FFFE para crear una dirección de 64 bits EUI-64 compatible tal como se presenta en la figura 4-1.

Para las direcciones multicast, una dirección IPv6 con una dirección destino multicast es transmitida a la dirección multicast Ethernet que comienza con el valor 3333H y termina con los últimos 4 octetos de la dirección DST. (El valor 3333H ocupa los 2 primeros octetos de la dirección multicast Ethernet, y los últimos 4 octetos de la dirección IPv6 de 16 octetos (designadas DST13, DST14, DST15 y DST16) ocupan los últimos 4 octetos de la dirección Ethernet.)

## 4.5. IPV6 SOBRE PPP

El protocolo PPP es usado extensivamente para la transmisión del tráfico TCP/IP sobre links de WAN. El soporte de IPv6 sobre PPP está documentado en RFC 2472. PPP consiste de 3 elementos: un formato de encapsulamiento (o marco) para links en serie; un Link Control Protocol (LCP) para establecer, configurar, y probar la conexión del link; y una familia de Network Control Protocols (NCPs) para establecer y configurar diferentes capas de los protocolos de red. Por ejemplo, el NCP para establecer y configurar IPv6 sobre PPP es llamado el protocolo IPv6 Control Protocol o IPV6CP.

El marco PPP es mostrado en la figura 4-2. Nótese que un paquete IPv6 o un paquete IPV6CP cabría dentro del campo de información de ese marco PPP. El campo Protocol define el tipo de paquete que es cargado: 0057H indica IPv6, mientras que 8057H indica IPV6CP.

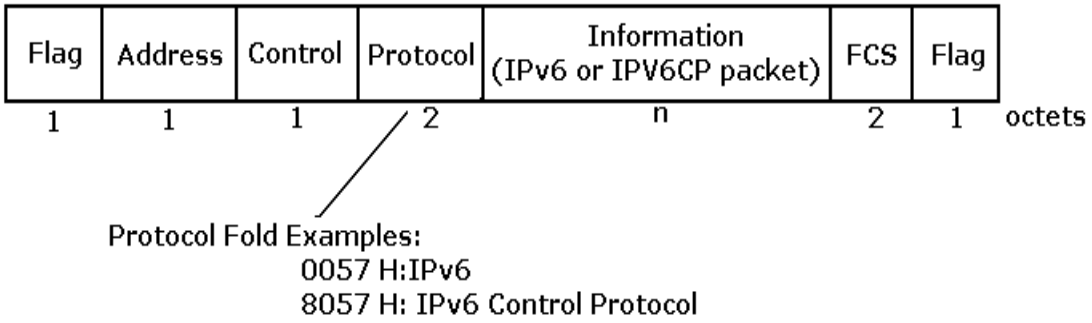



**Fig. 4-2. IPv6 sobre PPP.**

Para las LAN como Ethernet o token ring, el identificador de interfase usado con el proceso de Stateless Address Autoconfiguration es basado en la dirección del hardware, que es típicamente residente en el ROM o en la tarjeta de red. Para links PPP, el identificador de interfase puede ser seleccionado usando uno de los siguientes métodos (listados en el orden de preferencia):

1. Si un identificador global IEEE (EUI-48 o EUI-64) está disponible en cualquier parte del nodo, entonces esa dirección debe ser usada.

2. Si un identificador global IEEE no está disponible, entonces una fuente diferente de unicidad, como un número serial de la máquina, debe ser usado.

3. Si una buena fuente de unicidad no puede ser encontrada, un número aleatorio debe ser generado.

IPV6CP permite a los parámetros IPv6 ser negociados durante el inicio del link. Dos opciones, el Interface Identifier y el IPv6 Compression Protocol, han sido definidos. La opción Interface Identifier facilita la negociación de un identificador de interfase de 64 bits únicos para ese link, usando una de las 3 alternativas listadas arriba. La opción IPv6 -Compression-Protocol provee una manera de negociar el uso de un protocolo de compresión de paquetes IPv6.

Los valores corrientes para el campo IPv6 -Compression-Protocol son encontrados en el documento más reciente ”Assigned Numbers” (actualmente RFC 1700).

## 4.6. IPV6 SOBRE FRAME RELAY.

El soporte para IPv6 sobre redes FRAME RELAY es definido en RFC 2590, que se basa en RFC 2427, “Multiprotocol Interconnect over Frame Relay”.

Como en el caso de ATM, las redes frame relay son consideradas redes NBMA; así, la información proveída en RFC 2491 también se aplica.

Las redes frame relay son usadas para conectar endpoints, como hosts y routers, a través de una red de área amplia. Las conexiones son hechas por circuitos virtuales, que son identificados por un Data Link Connection Identifier (DLCI). El DLCI puede ser de 10, 17 o 23 bits de longitud. Cuando existen múltiples endpoints, los circuitos virtuales pueden formar una red completamente conectada (donde todos los endpoints están conectados a otros endpoints). Cada circuito virtual tiene sus propias características de transmisión, como rendimiento de

procesamiento de datos, tamaño de tramas (frame), y así. Dos tipos diferentes de circuitos virtuales son definidos: Permanent Virtual Circuits (PVCs), que son establecidos para asignaciones administrativas, o Switched Virtual Circuits (SVCs), que son establecidos dinámicamente.

El formato del marco del frame relay es derivado del formato del marco ISO High Level Data Link (HLDL), pero combina los campos HLDC Address y Control en un simple campo Address. El tamaño por defecto del marco de frame relay es 1,600 octetos, que permite 1,592 octetos como el tamaño por defecto MTU para IPv6 (sin contar los caracteres Flag que comienzan y terminan el marco).

El formato del campo de frame relay Address es definido en ITU-T Recommendation Q.922. Nótese que hay 2 posibles longitudes para este campo Dirección, 2 y 4 octetos. El campo de dirección de 2 octetos es usado por LCIs de 10 bits y el campo de dirección de 4 octetos es usado por DLCIs de 17 o 23 bits.

RFC 2590 define el método para construir el identificador de interfase para frame relay, usando 3 campos: el campo “EUI bits”, el campo ”Mid”, y el campo ”DLCI”. Además, el campo “Mid” puede ser construído en varias formas diferentes.

La opción Source/Target Link-Layer Address, que es usada en el proceso Neighbor Discovery. Se encuentran 2 tipos de direcciones de mapeo diferentes: una basada en el formato DLCI, y una segunda basada en el formato Frame Relay Address. Las especificaciones de estos formatos están definidas en detalle en RFC 2590.

Las extensiones al protocolo Neighbor Discovery en soporte de las redes frame relay. Estas extensiones son conocidas como Inverse Neighbor Discovery (IND), y permiten a un nodo frame relay descubrir el equivalente a las direcciones link-layer que identifican el nodo local de esta localización, y también identificar el nodo local de una localización remota (por ejemplo El otro extremo de una conexión virtual). El protocolo IND opera de forma similar a Neighbor Discovery, donde un nodo solicitando una dirección IP target transmite un mensaje de solicitud, y el nodo target responde con un anuncio que contenga la información solicitada.

## 4.7. MOBILE IPV6

En las redes locales que hemos discutido hasta ahora, todos los usuarios están asumidos a tener una conexión del hardware a la red, y mantener esta conexión por un cierto periodo de tiempo. Estudios recientes tratan con usuarios móviles y los temas particulares que sus configuraciones traen. Cada nodo móvil es siempre identificado por una dirección base sin importar sus accesorios actuales al

Internet. Cuando está lejos de su dirección base, está asociado con una dirección care-of, que provee detalles concernientes a su localización actual. Cualquier paquete IPv6 enviado a la dirección base sería entonces ruteado a la dirección care-of. Este proceso es igualmente aplicable a un usuario moviéndose de un segmento Ethernet a otro segmento Ethernet como a otro usuario moviéndose de un segmento Ethernet a una celda LAN sin cables.

La asociación entre la dirección base y la dirección care-of es llamada un binding para el nodo móvil. La dirección care-of puede ser obtenida usando la auto configuración de dirección sin estado o con estado (DHCPv6), de acuerdo al protocolo Neighbor Discovery. El registro del binding es realizado por el nodo móvil que envía un paquete conteniendo una opción destino Binding Update al agente base, que responde con un Binding Acknowledgement al nodo móvil.

Como se puede esperar, el soporte para movilidad de nodos abarca un número de procesos IPv6, incluyendo nuevas opciones IPv6, modificaciones al protocolo Neighbor Discovery, recepción de mensajes ICMPv6, consideraciones de seguridad, y otros.

## 4.8. DIRECCIONES IEEE EUI-64

El Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) administra el esquema de direccionamiento para todas las redes locales que se adhieren a las series de estándares IEEE Proyecto 802. Esto incluye las redes CSMA/CD, como IEEE 802.3, 10BASE-T ó IEEE 802.5 Token Ring.

Una dirección IEEE 802 consiste de dos partes: un ID de la Compañía y un ID de Extensión. La IEEE asigna IDs de Compañía (a veces llamada IDs de los manufacturados) a organizaciones que manufacturan periféricos de hardware de red. La compañía, a su vez, asigna el ID de Extensión (a veces llamado el ID de Tarjeta). Unidos, el ID de la Compañía y el ID de Extensión se convierten en un identificador único (o numero serial) para este hardware de red; es típicamente grabado en la memoria ROM de la tarjeta de red, llamada comúnmente MAC o dirección física.

En el pasado, el IEEE había puesto 24 bits al ID de la Compañía y 24 bits al ID de Extensión, resultando en una dirección de 48 bits. La IEEE recientemente mejorado este esquema de direccionamiento para expandir el campo de los ID de Extensión a 40 bits, acomodando así mas interfaces de hardware (aproximadamente 1 trillón – 1012) por manufacturado. Este nuevo esquema, al cual provee direcciones de 64 bits de largo, es llamado EUI-64.

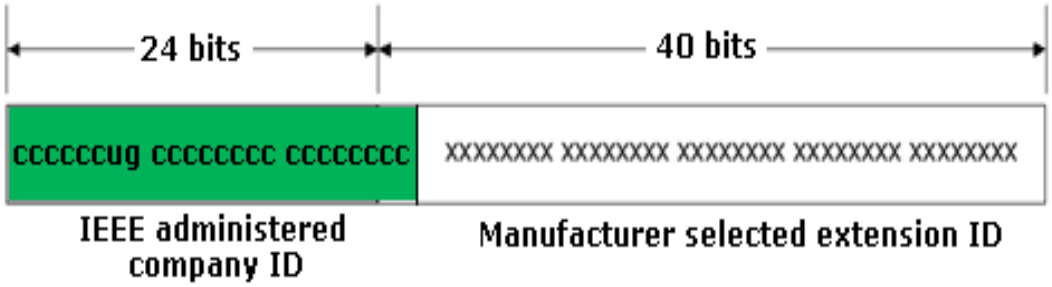



**Fig. 4-3. Direcciones IEEE EUI-64.**

En el esquema de direccionamiento IEEE (ambos 48-bits y EUI-64), hay dos bits de flag: el bit Individual/Grupo (I/G) y el BIT Universal/Local (U/L). Estos bits de flag identifican si es una Dirección Individual (I/G = 0), una Dirección de Grupo (I/G = 1), administrada Universalmente (o globalmente) (U/L = 0), o administrada Localmente (U/L = 1).

Muchas de las direcciones IPv6 incorporan un campo de ID de Interface, el cual es definido usando el formato EUI-64. La dirección EUI-64 con significado universal (o global) es ilustrada en la Figura (Nótese el séptimo BIT del primer octeto: U/L=0). La dirección EUI-64 con un significado local (usado para identificadores de interfaces en enlaces o nodos con IPv6) es ilustrada en la figura. Nótese que, en este caso, el séptimo BIT del primer octeto ha sido invertido (U/L = 1).

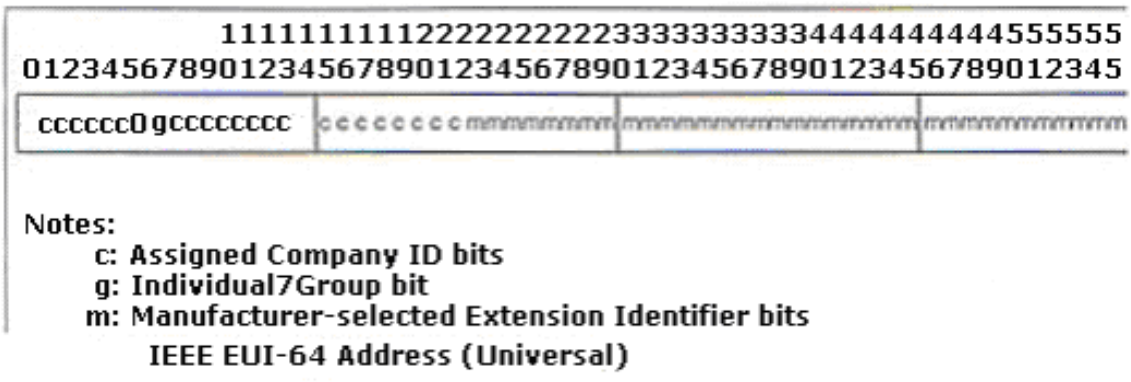



**Fig. 4-4. Direcciones IEEE EUI-64. (Universal)**

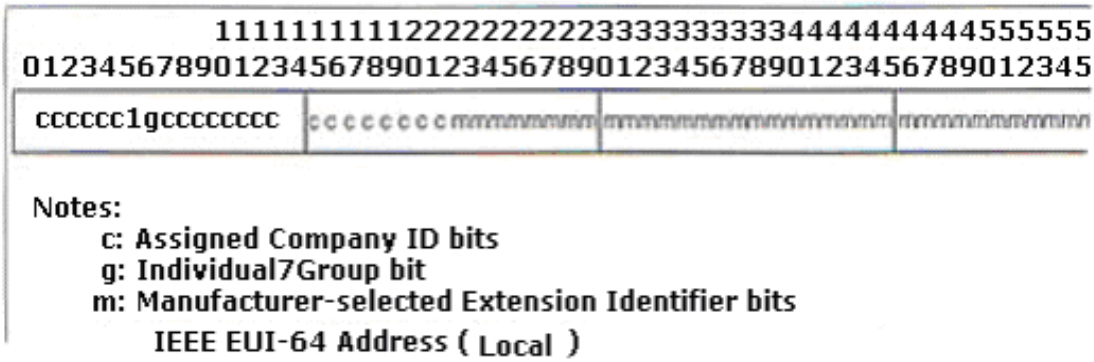



**Fig. 4-5. Direcciones IEEE EUI-64. (Local)**

Para convertir la dirección de 48 bits a la dirección EUI-64, se insertan 16 bits entre él ID de Compañía y el ID de Extensión. Estos 16 bits son representados por los caracteres hexadecimales FFFE, o 1111 1111 1111 1110 en binario, entre el ID de la Compañía (bits c) y el ID de Extensión definido por el manufacturado (bits m). En la figura 4-4 se muestra el esquema de las direcciones EUI-64.

Algunas interfaces, como AppleTalk y ARCnet, no se adhieren al esquema de direccionamiento IEEE. Para crear un identificador con el formato EUI-64 para este tipo de enlaces, el identificador de nodo es colocado en los bits de más a la derecha, y todos ceros a la izquierda. En este caso, U/L = 0, indicando una dirección de alcance local.

# CAPITULO V

# CAPITULO V: PROTOCOLOS DE ENRUTAMIENTO, ICMPv6, NEIGHBOR DISCOVERY PROTOCOL.

## 5.1. PROCESO DE RUTEO.

En este capítulo nos se analizará una capa más arriba y se considerarán temas específicos a los procesos de ruteo en la capa de Red OSI. Pero primero, algunas definiciones:

Un sistema autónomo (AS) es una red que es administrada por una simple entidad. Los protocolos de ruteo caen en 2 categorías generales: Interior Gateway Protocols, o IGPs, y Exterior Gateway Protocols, o EGPs. Un IGP es usado para transportar información de ruteo como un AS, mientras que un EGP es usado para transportar información de ruteo entre más de un AS.

El Routing Information Protocol (RIP), ha sido realzado para soportar IPv6. Además, los realces de IPv6 han sido propuestos para otro IGP, el protocolo Open Shortest Path First (OSPF). Los realces de un EGP, el Border Gateway Protocol (BGP), también han sido propuestos. Comenzaremos nuestro estudio por considerar cambios a RIP.

## 5.2. ROUTING INFORMATION PROTOCOL (RIP).

Routing Information Protocol es uno de los IGP más ampliamente usados; fue originalmente definido en 1988 y documentado en RFC 1058. Soporte para RIP con IPv6 es llamado RIPng y está documentado en RFC 2080.

RIP es un protocolo basado en el Algoritmo Vector-Distancia, con una historia que empieza en los días tempranos del ARPAnet. RIP está diseñado para redes de tamaño moderado, con unas pocas limitaciones:

- El protocolo es limitado a redes cuya parte más larga (para diámetro de red) es 15 saltos (hops).

- El protocolo depende de un proceso llamado “contar hasta el infinito” para resolver ciertas situaciones, como loops de ruteo. Este proceso puede consumir una gran cantidad de ancho de banda de red antes de la resolución.

- El protocolo depende de medidas fijas para comparar rutas alternativas, sin importar los parámetros en tiempo real como tardanza, confiabilidad o carga.

RIPng es el protocolo que permite a los routers intercambiar información para computar rutas a través de una red basada en IPv6. Cada router que implementa RIPng es asumida a tener una tabla de ruteo que tiene una entrada para cada destino IPv6 alcanzable. Cada entrada contiene lo siguiente:

- El prefijo IPv6 del destino.
- Una medida que indica el costo total de obtener un datagrama desde el router hasta el destino.
- La dirección IPv6 del próximo router en el camino al destino, llamado el próximo salto (hop).
- Un Router Change Flag que indica si la información acerca de esa ruta ha cambiado recientemente.
- Varios relojes (timers), como un reloj de 30 segundos que apunte la transmisión de la información de la tabla de ruteo a los routers vecinos.

RIPng es un protocolo basado en User Datagram Protocol (UDP) que envía y recibe paquetes en el puerto UDP # 521. El paquete RIPng incluye 3 campos: Command (Request o Response), Version (1) y Route Table Entry (RTE). Cada RTE incluye el prefijo IPv6, el Route Tag (para separar rutas internas de las externas), un campo Prefix Length (para determinar el número de bits significantes en el prefijo), y Metric (para definir la medida corriente para el destino).

RIPng también provee la habilidad de especificar el próximo salto inmediato de dirección IPv6 para paquetes. Este próximo salto está especificado por un RTE especial, The Next Hop Route Table Entry. Next Hop RTE está identificado por el valor de FFH en el campo Metric. El campo Prefix especifica la dirección IPv6 del próximo salto; Route Tag y Prefix Length son configurados a cero en la transmisión e ignorados en la recepción.

La versión 1 de RIPng soporta 2 comandos: Request y Response. Un Request es utilizado para preguntar por toda o parte de la tabla de ruteo. En muchos casos, los Request son enviados como multicasts desde el puerto RIPng (521). Si la información para solo un router es necesitada, esa solicitud sería enviada directamente a ese router desde un puerto que no sea el puerto RIPng. Hay 3

tipos de Response: una respuesta a un query específico; una actualización regular, que es una respuesta no solicitada enviada cada 30 segundos a todos los routers vecinos; y una actualización accionada causada por un cambio de ruta. Detalles específicos concernientes al proceso de paquetes en Request y Response son dados en RFC 2080.

Las figuras 5-1 y 5-2 presentan el formato de RIPng y RTE respectivamente:

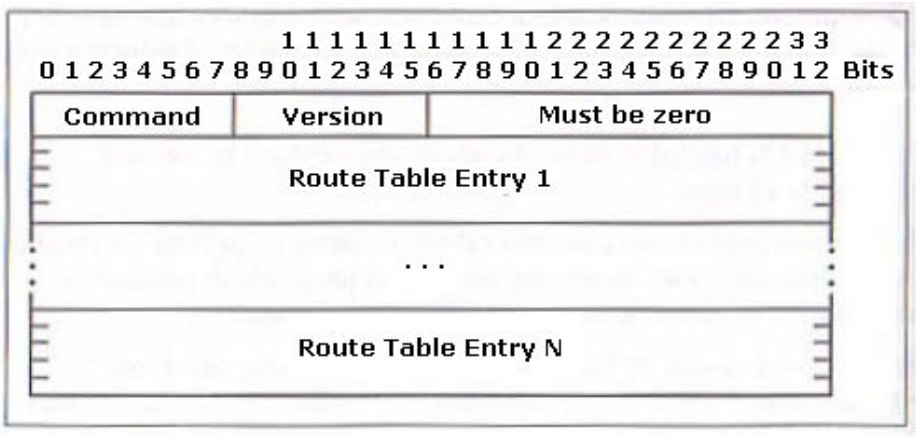



**Fig. 5-1. Formato del Paquete RIPng.**

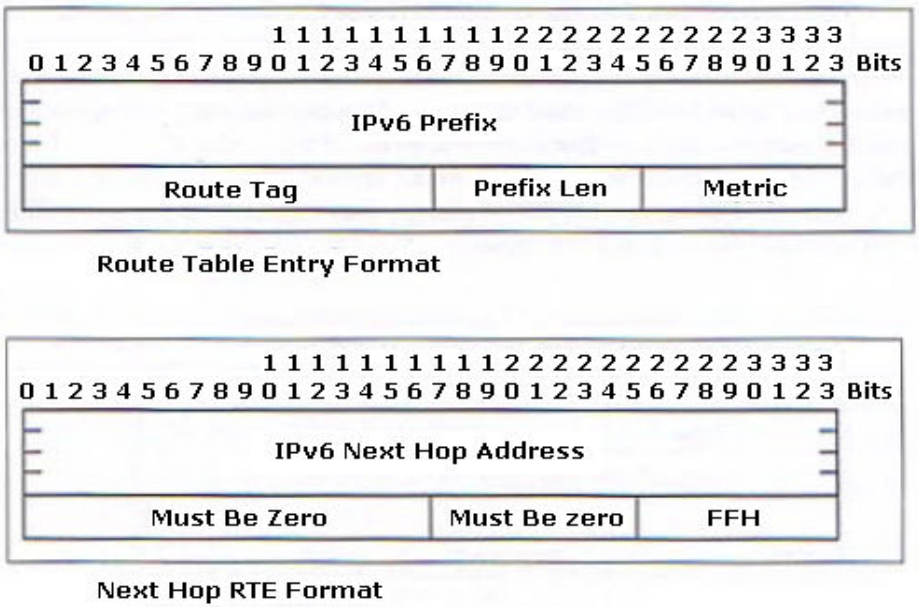



**Fig. 5-2. Formato RTE.**

## 5.3. OPEN SHORTEST PATH FIRST PROTOCOL (OSPF).

El protocolo Open Shortest Path First Protocol - Primero la Ruta Mas Corta - (OSPF) opera usando un algoritmo Link State Algorithm (LSA) y está definido en RFC 2328. Un LSA ofrece varias ventajas sobre un algoritmo Distance Vector Algorithm, como el que es usado con RIP. Estas incluyen la habilidad de hacer lo siguiente: configurar topologías jerárquicas (en vez de planas); adaptación más rápida a los cambios en los trabajos de Internet; permisos para trabajos de Internet muy grandes; calcular múltiples rutas con costo mínimo que permitan que la carga de tráfico sea balanceada sobre varios caminos; y permitir el uso de máscaras de subred de longitud variable. Además, la versión actual de OSPF (versión 2), definida en RFC 2328, soporta IPv4 e incluye la habilidad de autentificar la fuente de los datos.

Hay 5 tipos de paquetes definidos para OSPF: Hello, Database Description, Link State Request, Link State Update y Link State Acknowledgement. La propuesta actual para OSPF para IPv6 sugiere que estos tipos de paquetes tengan un encabezado consistente. La diferencia más notable entre este encabezado propuesto y el actualmente definido para OSPF para IPv4 es la ausencia del campo Authentification. Como IPv6 tiene su propio header Authentification disponible, esa función es removida del encabezado de OSPF para IPv6 para evitar redundancia; esto se muestra en la figura 5-3:

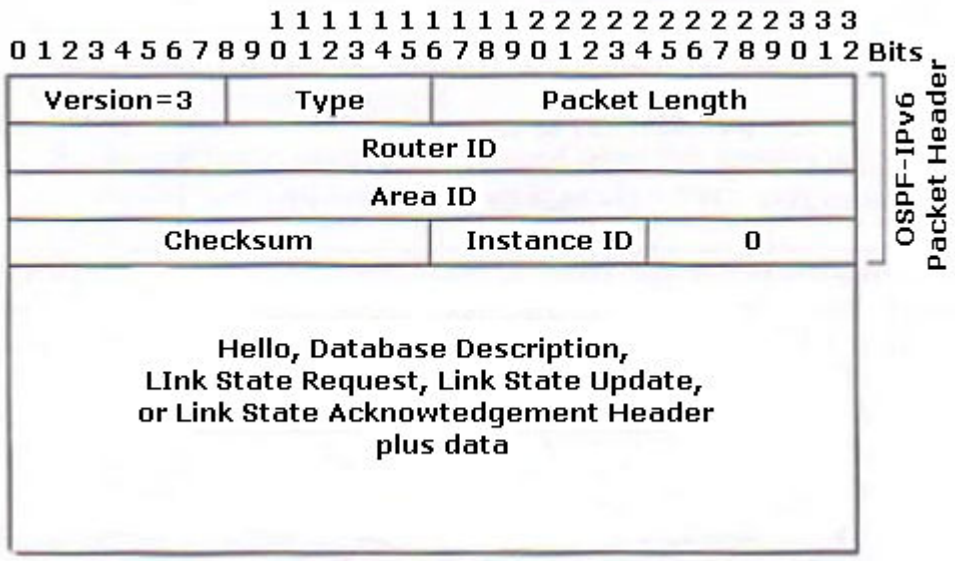



**Fig. 5-3 Paquetes definidos para OSPF.**

Algunos cambios adicionales a OSPF han sido propuestos para proveer soporte para IPv6. Entre estos cambios están:

- Procesamiento de protocolo en una base “por link”, no en base a “por subred”, desde múltiples subredes se les puede asignar un link con IPv6. (Recordar que RFC 2460 define un link IPv6 como “una facilidad de comunicación o medio sobre el cual los nodos se pueden comunicar a la capa de link”.)

- Retiro de semántica de direccionamiento desde los encabezados de paquetes OSPF, dejando un núcleo de red independiente de protocolos. Por ejemplo, las direcciones IPv6 no son cargadas en los paquetes SPF, con la excepción de las cargas útiles Link State Advertisement cargadas en los paquetes Link State Update.

- Nuevo Flooding Scope para los Link State Advertisement (alcance link-local).

- Soporte para ejecutar múltiples instancias de protocolo OSPF por link.

- Uso de direcciones Link-Local, que no son reenviadas por los routers.

- Retiro de la autentificación del encabezado de paquetes OSPF, puesto que esta función es ahora cubierta con los encabezados de IPv6 Authentification y Encapsulating Security Payload.

- Cambios en el formato de paquetes: nuevo número de versión (3), retiro del campo Authentification, y así.

- Nuevos formatos Link State Advertisement para distribuir la resolución y próximo salto de resolución de la dirección IPv6, más nuevos procesos para manejar tipos de LSA desconocidos.

- Soporte actualizado para stub de áreas.

- Identificación consistente de todos los routers vecinos en un link dado por sus ID de router OSPF.

- Retiro de la semántica de Type of Service (ToS), con la provisión de que el campo IPv6 Flow Label puede ser usado para esta función en el futuro.

## 5.4. BORDER GATEWAY PROTOCOL (BGP).

Un sistema autónomo intercambia información de ruteo con otro sistema autónomo usando un EGP. El más prevaleciente es Border Gateway Protocol (BGP), que ha ido a través de varias iteraciones. Estas incluyen BGP-1 (RFC 1105), BGP-2 (RFC 1163), BGP-3 (RFC 1267) y BGP-4 (RFCs 1771, 1772, 773 y 1774). La función primaria de un sistema BGP es intercambiar información de como alcanzar la red con otros sistemas BGP. Esta información incluye datos en la lista de los AS que esta información atraviese, que permite la construcción de un gráfico de conectividad.

BGP-4 usa el TCP para mayor confiabilidad de comunicación entre los AS. El encabezado del mensaje BGP-4 está definido en RFC 1771. Este encabezado tiene 19 octetos de longitud y soporta uno de 4 tipos de mensajes:

- ✓ **OPEN:** inicia la conexión BGP.
- ✓ **UPDATE:** usado para transferir información de ruteo entre puntos BGP.
- ✓ **KEEPALIVE:** intercambiado en una base periódica para determinar como alcanzar los puntos.
- ✓ **NOTIFICATION:** enviado cuando una condición de error es detectada; causa que la conexión BGP sea cerrada.

Después que una conexión TCP es establecida, el primer mensaje enviado es un mensaje OPEN. Si el OPEN es aceptable al otro lado de la conexión, un mensaje KEEPALIVE es retornado en confirmación. Cuando el OPEN ha sido confirmado, los mensajes UPDATE, KEEPALIVE y NOTIFICATION pueden ser intercambiados. La figura 5-4 muestra el mensaje de cabecera:

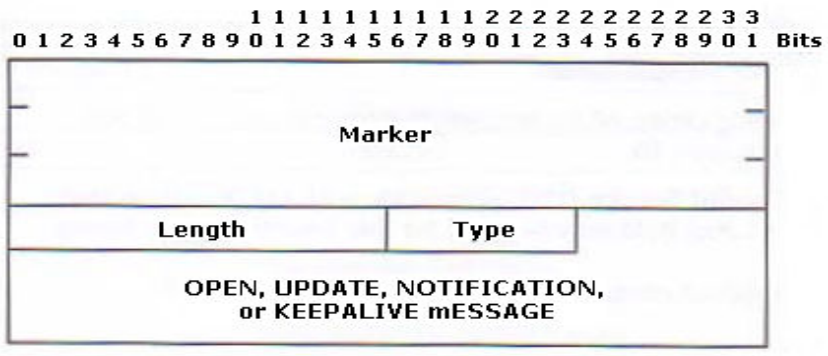



**Fig. 5-4. BGP- 4 Mensaje de Cabecera.**

Extensiones multiprotocolos para BGP-4 han sido definidas en RFC 2283 que le permiten cargar múltiples protocolos de capa de red (network layer), incluyendo IPv6. Como con otros cambios a los protocolos de ruteo, estas extensiones BGP-4 deben incluir soporte para la estructura de direccionamiento IPv6, la habilidad para distinguir entre varios protocolos de capa de red, y así.

Detalles concernientes al uso de estas extensiones de protocolos son documentados en RFC 2545.

## 5.5. CAMBIO DE RUTEO ADICIONALES PROPUESTO PARA IPV6.

A este tiempo presente, varios cambios de ruteo adicionales han sido propuestos en soporte de IPv6. Un nuevo mecanismo llamado Router Renumbering (RR) permite a los prefijos de direcciones en los routers ser fácilmente configurados o reconfigurados. Este mecanismo provee medios a un administrador de red para hacer actualizaciones a los prefijos usados y anunciados por los routers IPv6 a través de un site. Los mensajes RR son un tipo especial de mensaje ICMP, con 2 códigos: Comandos (commands), que son enviados a los routers; y Resultados (results), que son enviados por los routers. Los mensajes RR son cargados en mensajes ICMPv6, con el ICMPv6 Type = 138. Los mensajes comparten un encabezado RR común, con distintos cuerpos de mensajes. Los mensajes Command incluyen los prefijos a ser modificados, mientras que los mensajes Result confirman la operación del prefijo.

Un nuevo tipo de Hop-by-Hop Option ha sido propuesto que alerte a los routers en tránsito a examinar los contenidos de un paquete IPv6. Esta opción es llamada Router Alert Option y está documentada en RFC 2711. En algunos casos, protocolos de control, como el Resource Reservation Reservation Protocol (RSVP), contienen información que necesita ser examinada y posiblemente actualizada por los routers en el camino desde la fuente inicial al destino último. Router Alert Option, cargada en un encabezado Hop-by-Hop Extension, envía señales a estos routers para examinar este paquete más cercanamente. El valor del campo de la opción identifica el tipo de protocolo contenido en el paquete (ICMPv6 Group Membership, RSVP, etc.) que requiere atención especial.

## 5.6. ICMPv6

El Internet Control Messages Protocol (56 en el campo de Next Header), tiene el mismo uso que su antepasado, el ICMPv4. La misión de un ICMP, es sobre todo la de informar. A continuación se explicará qué, cómo y de que forma cumple con su trabajo.

### 5.6.1. TIPOS DE ICMPV6 Y FORMATO

Los mensajes de ICMP, se han dividido en 2 clases, los que comunican errores, y los que piden y dan información sobre un nodo. Para diferenciarlos, se han adjudicado una numeración del 0 al 127 a los mensajes que contienen información y del 128 al 255, sobre los que informan de algún tipo de error de una petición.

Un paquete ICMPv6, esta formado por una cabecera IPv6, y es precedido inmediatamente por una cabecera con valor 58 en el campo next header.

Nótese, que este procedimiento es diferente al de IPv4, y que un ICMP puede ser insertado en cualquier tipo de paquetes.

### 5.6.2. TIPOS DE INFORMACIÓN DE PAQUETES ICMPV6.

Los mensajes de información, pueden ser del tipo:

#### 5.6.2.1. Echo Request (Type 128).

Un nodo, puede enviar un ICMP Echo Request (Más conocidos como pings), para saber el tiempo de respuesta de otro host.

Los valores de los siguientes campos son:

**Type:** 128
**Code:** 0
**Checksum:** Suma de control, para la comprobación de la información.
**Identifier:** identificador para contrastar los ICMP Echo Reply de respuesta.
**Sequence Number:** Secuencia de números, para contrastar los ICMP Echo Reply de Respuesta en orden.
**Data:** Datos aleatorios o ceros de relleno.

La recepción de ICMP Echo Request, debe ser comunicada a la capa superior de trasporte.

#### 5.6.2.2. Echo Reply (Type 129)

El ICMP Echo Reply, es enviado como respuesta a un ICMP Echo Request. El ICMP Echo Reply debe ser trasportado al proceso que origino el ICMP Echo Request.

Los valores de los siguientes campos son:

**Type:** 129
**Code:** 0
**Checksum:** Suma de control, para la comprobación de la información.
**Identifier:** identificador que debe contrastar con los ICMP Echo request que se han recibido.
**Sequence Number:** Secuencia de números, que debe contrastar con los ICMP Echo request que se han recibido en el mismo orden.
**Data:** Datos aleatorios o ceros de relleno.

### 5.6.3. MENSAJE DE ERRORES EN ICMPV6.

#### 5.6.3.1 Destination Unreachable (Type 1).

Un ICMP Destination Unreachable es mandado por un router, o por cualquier nodo, para informar de la imposibilidad de que un paquete llegue a su destino.

No se deberían mandar ICMPv6, si son ocasionados por problemas de congestión de la red. Estos ICMP se dividen en subclases, según el tipo de problema que haya ocasionado su emisión:

- Si el error es ocasionado por un envió de un paquete al nodo erróneo, este enviara un ICMPv6 con código 0.

- Si el error es ocasionado por un envió hacia un destino cerrado por causas administrativas (Un firewall por ejemplo), se debe enviar un ICMP de código 1.

- Si el error es ocasionado por la imposibilidad de resolver la dirección IP de un link, se enviara un ICMPv6 con código 3.

- Si el error es ocasionado por un fallo en la capa de trasporte si el puerto esta indisponible para la misma se enviara un ICMP con código 4. Por ejemplo, un paquete TCP enviado a un puerto UDP.

Un nodo que ha recibido un ICMPv6 Destination Unreachable, debe comunicarlo a la capa superior del proceso.

Los valores de los siguientes campos son:

**Type:** 0
**Code:** 0 - no route to destination
1 - communication with destination administratively prohibited
2 - (not assigned)
3 - address unreachable
4 - port unreachable
**Unused:** Campo sin uso, que debe ser inicializado a 0 por el emisor e ignorado por el destino.
**Checksum:** Suma de control, para la comprobación de la información.

#### 5.6.3.2. Packet Too Big (Type 2)

Un ICMP Packet Too Big, es enviado cuando el tamaño máximo de un paquete es superior a la MTU de la interfaz de red a la que se ha enviado.

También es enviado por un router, si el siguiente salto tiene un MTU inferior al tamaño del paquete. Este ICMP, puede ser usado para saber el MTU de una ruta.

Los valores de los siguientes campos son:

**Type:** 2
**Code:** 0 (Inicializado a 0 por el origen, ignorado por el destino)
**Checksum:** Suma de control, para la comprobación de la información.
**MTU:** MTU del siguiente salto.

#### 5.6.3.3. Time Exceeded (Type 3)

Si un router recibe un paquete con el Hop limit a 0 o si es el quien lo tiene que poner a 0, el paquete es descartado y se envía un ICMPv6 Time Exceeded.

Si un host, no puede ensamblar un paquete en un tiempo x, descartara todos los fragmentos recibidos y también enviara un ICMP de esta clase. La llegada de un ICMPv6, debe ser notificada a la capa superior de trasporte.

Los valores de los siguientes campos son:

**Type:** 3
**Code:** 0 - Hop Limit exceeded in Transit (Rebasado el limite de saltos)
1 - Fragment Reassembly Time Exceeded (Rebasado el tiempo de ensamblado en destino).
**Unused:** Campo inicializado a 0 en origen, e ignorado por destino.

**Checksum:** Suma de control, para la comprobación de la información.

#### 5.6.3.4. Parameter Problem (Type 4)

Si un nodo IPv6, al procesar un paquete, encuentra un error en uno de los parámetros de sus campos, enviara un ICMP Parameter Problem informando al destino de la situación del error en el paquete.

Los valores de los siguientes campos son:

**Type:** 4
**Code:** 0 - Error header field encountered (Error en la cabecera)
1 - Unrecognized Next Header type encountered (Numero de Next Header desconocido).
2 - Unrecognized IPv6 Option Encountered (Opción desconocida en el paquete IPv6).
**Checksum:** Suma de control, para la comprobación de la información.
**Pointer:** Contiene un offset, para la localización del parámetro que origino el error. El offset, es el byte donde se encuentra el dato erróneo dentro del paquete.

### 5.6.4. Seguridad en ICMPv6

Los ataques producidos por los ICMP enviados de forma masiva, generalmente para provocar un DoS (Denial of Service) y/o la caída de un nodo de una red y/o de una conexión, son lo suficientemente conocidos como para no tener que volver a explicarlos. El protocolo IPv6, implementa medios de autentificación que pueden evitar los más comunes.

- Caída por recepción de envíos masivos de ICMP.
- Desconexión de un host, por él envió de un atacante al servidor, de ICMP con mensajes de error.
- Falsificación de ICMP.

Todos estos problemas, están descritos en el RFC 2463, así como sus posibles soluciones mediante aplicaciones de métodos autentificadotes al nivel de trasporte IP y/o mediante el checksum de control.

## 5.7. NEIGHBOR DISCOVERY (NDP)

El Neighbor Discovery Protocol (protocolo de descubrimiento de vecindad), es el encargado de saber por que hosts/redes estamos rodeados. Esto, también incluye descubrir las características del medio por donde van a circular los paquetes que salgan de nuestra maquina. El Neighbor Discovery hace uso de ICMPv6, para comunicarse. Tal y como se comenta en el RFC 2461, el Neighbor Discovery, es una combinación de ARP, ICMP Router Discovery e ICMP redirect, y a su vez se han incorporado nuevas funciones. Entre las funciones de este protocolo, están las de:

- ✓ **Router Discovery (Descubrimiento de router):** Comunica al host y a otros routers, la existencia de un nuevo router, o la permanencia / eliminación de los actuales.

- ✓ **Parameter Discovery (Descubrimiento de parámetros**): Da información a los nodos de una red, sobre el MTU, así como del número máximo de saltos para llegar al exterior.

- ✓ **Prefix Discovery (Descubrimiento de prefijo):** Comunica al nodo el prefijo de la red, que tiene la dirección IPv6 de su subred.

- ✓ **Next-hop determination (Determinación del próximo salto):** Comunica el nodo más cercano. Este valor puede ser usado para determinar la ruta más corta por la cual se encaminaran los paquetes.

- ✓ **Address Autoconfiguration (Auto configuración de dirección):** Da a conocer a la maquina, la IP de un interfaz de red.

- ✓ **Address resolution (Resolución de dirección):** Se encarga de establecer la correspondencia entre la dirección IP y la de su capa de enlace (Dirección MAC de una ethernet por ejemplo).

- ✓ **Neighbor Unreachability Detection (Detección de inaccesibilidad de un vecino):** Detecta la caída, o eliminación de un router y/o host.

- ✓ **Duplicate Address Detection (Detección de Duplicidad de direcciones):** Comprueba que no hay direcciones IP duplicadas dentro de una red. Puede ser usado antes de dar de alta un nuevo nodo.

- ✓ **Redirect (Redirección):** Informa a un nodo, del mejor camino mas corto, para alcanzar un destino.

### 5.7.1. FORMATOS PARA NEIGHBOR DISCOVERY. INALCANZABLE

Los formatos para los mensajes, quedan definidos de la siguiente manera:

#### 5.7.1.1. Router Solicitation:

Los valores para estos campos, son los siguientes:

**Type:** 133
**Code:** 0
**Checksum:** (Suma de control ICMPv6)
**Reserved:** 0 (Sin un valor asignado)
**Options:**
**-Source link-layer address:** Dirección de la capa de enlace del origen del mensaje.

#### 5.7.1.2. Router Advertisement:

Los valores para estos campos, son los siguientes:

**Type:** 134
**Code:** 0
**Checksum:** (Suma de control ICMPv6)
**Cur Hop Limit:** Valor actual que debe tomar el campo de IP que indica el numero de saltos por defecto, o Hop Limit, especificado en 8 bytes unsigned integer. Un valor de 0, no especifica nada.
**M:** Flag de 1 bit, para el Managed address configuration.
**O:** Flag de 1 bit, para el Other stateful configuration.
**Reserved:** Campo reservado para usos futuros. Con valor de 6 bit, debe ser inicializado a 0. Cualquier otro valor, será ignorado.
**Router Lifetime:** Valor de 16 bits unsigned integer. El tiempo de vida del Router por defecto. Si el valor es 0, no debe ser usado para este fin.
**Reachable Time:** Tiempo medido en 32 bits unsigned integer, que indica, en milisegundos, el tiempo desde que un nodo, ha recibido una confirmación de alcance, por parte de sus vecinos. Un valor de 0, no especifica nada.
**Retrans Timer:** Tiempo en milisegundos, expresados como unsigned integer, trascurrido entre 2 mensajes de solicitud de vecindad. Un valor de 0, inhabilita este campo.
**Options:**
**- Source link-layer address:** Dirección de la capa de enlace del origen del mensaje.

**- MTU:** Debe ser enviada en redes con la MTU variable. En otra clase de enlaces, esta opción es opcional.
**- Prefix Information:** Los prefijos de las redes que alcanza el router excepto la local.

#### 5.7.1.3. Neighbor Solicitation

Los valores para estos campos, son los siguientes:

**Type:** 135
**Code:** 0
**Checksum:** (Suma de control ICMPv6)
**Reserved:** 0 (Sin un valor asignado)
**Target Address:** Dirección IP hacia la cual se envía la solicitud. Este campo no debe ser ocupado por una dirección de multicast.
**Options:**
**- Source link-layer address:** Dirección de la capa de enlace del origen del mensaje. No debe incluirse si es una dirección de arranque. En cambio si ya tiene IP, puede ser incluida si es una solicitud de multicast y debe ser incluida si es una solicitud de anycast.

#### 5.7.1.4. Neighbor Advertisement

Los valores para estos campos, son los siguientes:

**Type:** 136
**Code:** 0
**Checksum:** (Suma de control ICMPv6)
**R:** Router flag de un bit. Indica que el nodo de envío es un router. Es usado por el Neighbor Unreachability Detection, para ver si un router cambia a host.
**S:** Solicited flag de un bit. Toma valor 1, si el mensaje es en respuesta a una solicitud de vecindad.
**O:** Override flag. Con valor 1, indica que la caché de destino debe ser actualizada. Si el valor es 0, la caché de destino no debe ser actualizada menos para los nodos implicados.
**Reserved:** 29 bits sin uso, destinados a futuras implementaciones. Debe ser inicializado a 0. Otro valor, será ignorado.
**Target Address:** Dirección de destino, que debe ser la del nodo que solicito este mensaje. No debe ser ninguna dirección de multicast.
**Options:**

**- Target link-layer address**: Dirección de la capa de enlace del destino. Puede ser incluida respondiendo a una solicitud de multicast y debe ser incluida si es una respuesta a una solicitud de anycast.

#### 5.7.1.5. Redirect

Los valores para estos campos, son los siguientes:

**Type:** 137
**Code:** 0
**Checksum:** (Suma de control ICMPv6)
**Reserved:** 0 (Sin un valor asignado)
**Target Address:** Informa al host, de que hay un camino mejor por donde encaminar su trafico hacia su destino, indicándolo en este campo.
**Destination Address:** Aquí informa el router al host, el destino del tráfico al cual se refiere.
**Options:**
**- Target link-layer address:** Dirección de la capa de enlace del destino. Debe incluirse si es posible. En enlaces del tipo NBMA (non-broadcast multi-access), los host podría requerir la dirección de la capa de enlace del destino.
**- Redirected Header:** Incluir tanto como sea posible de la cabecera IP del paquete que ha provocado el envío del mensaje.

### 5.7.2. FORMATO DEL CAMPO DE OPCIONES DEL NEIGHBOR DISCOVERY.

Dentro de los mensajes anteriormente citados, el campo Options debe tener el formato que se muestra en la figura 5-5:

- ✓ Source/Target Link-layer Address

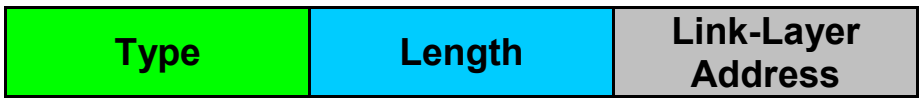



**Fig. 5-5. Formato para el Campo Options.**

**Type:** 1 Para el Source Link-layer Address
2 Para el Target Link-layer Address

**Length:** Longitud, incluyendo el campo Type y Length medida en valores de 8 bytes.
**Link-Layer Address:** Dirección de la capa de enlace. Su formato esta a la espera de ser especificado.

#### 5.7.2.1. Prefix Information

**Type:** 3
**Length:** 4
**Prefix Length:** 8 bits de unsigned integer en un rango de 0 a 128 que indican las primeras posiciones del prefijo que son validas.
**L:** Flag de on-link. Con valor 1, indica que la dirección es del tipo on-link, a 0, no especifica nada.
**A:** Flag de autonomous address-configuration (configuración autónoma de configuración). Con valor 1, indica que el prefijo puede ser usado para que el host configure su dirección.
**Reserved1:** Campo de 6 bits reservados para uso futuro. Se debe inicializar a 0.
**Valid Lifetime:** Valor de 32 bits insigned integer, que informa del tiempo en segundos que el prefijo, a fines de direcciones on-link, debe ser valido. Si el campo son todos 1 (0xffffffff) el valor es infinito.
**Preferred Lifetime:** Valor de 32 bits insigned integer, que indica el tiempo en segundos, que la dirección generada a partir del prefijo es preferible que sea usada. Si el campo son todos 1 (0xffffffff) el valor es infinito.
**Reserved2:** Campo reservado para uso futuro. Se debe inicializar a 0.
**Prefix:** Contiene una dirección IP o un prefijo IP. El campo Prefix Length contiene los bits primeros a tener en cuenta y el resto deben ser inicializados a 0 e ignorados por el que envía el mensaje. Un router no debe mandar prefijos hacia links locales y un host local, debe ignorarlo.

#### 5.7.2.2. Redirected Header

**Type:** 4
**Length:** longitud en unidades de 8 bytes de la opción.
**Reserved:** Campo reservado para futuros usos. Debe ser inicializado a 0.
**IP header + data:** Paquete original truncando su tamaño para que, la longitud total, no exceda de 1280 bits.

#### 5.7.2.3. MTU

**Type:** 5

**Length:** 1
**Reserved:** Campo reservado para futuros usos. Debe ser inicializado a 0.
**MTU:** 32 bits unsigned integer que indica el MTU recomendado. El valor debe ser aplicado a todos los segmentos.

Si algún campo de opciones es encontrado dentro de un tipo de mensaje que no le corresponde, debe ser simplemente ignorado por el router.

El Neighbor Discovery, es un protocolo tan extenso, que ocupa un RFC entero (el RFC 2461).

# CAPITULO VI

# CAPITULO VI: MOVILIDAD

## 6.1. OPERACIÓN DE MOVILIDAD.

Todo nodo móvil (Mobile Node, MN) tendrá una dirección 'de casa' (Home Address, HA), que será su dirección en su red origen. Esta dirección se mantendrá aunque se cambie de red. Los paquetes que se envíen al nodo móvil estando éste en su red origen serán encaminados de forma normal, como si el soporte de movilidad no existiese.

En el momento en que el nodo móvil pase a una red que no sea la suya de origen, éste obtendrá una nueva dirección 'de invitado' (Care-of-Address, CoA). A partir de ahora el nodo podrá ser contactado también a través de esta CoA. Lo siguiente que hará el nodo móvil es contactar un router de su red de origen (Home Agent HA) y comunicarle cual es su CoA actual. De esta forma, cuando un paquete sea enviado a la 'dirección de casa', el router sabrá que tendrá que interceptarlo y reenviarlo con destino a la CoA del nodo móvil.

Lo que en realidad hace el MN cuando se mueve es mandar un mensaje de Binding Update (BU) al HA. El BU asocia la CoA con la dirección 'de casa' del nodo móvil durante un cierto periodo de tiempo.

Llamaremos nodo correspondiente (Correspondent Nodo, CN) a cualquier nodo, ya sea fijo o móvil que se comunique con un MN.

Cuando un nodo móvil se comunica con un CN, el MN envía directamente los paquetes utilizando la dirección 'de invitado' que ha obtenido en la red que se encuentre. Sin embargo, el CN envía los paquetes a la dirección 'de casa' del MN, que serán interceptados por Hay reenviados a la CoA de nodo móvil. Tendríamos un caso de ruta triangular, que no es ningún problema, pero es ineficiente. Para resolver esto, MobileIPv6 presenta el concepto de optimización de ruta. Este mecanismo permite al MN avisar al CN de que puede enviarle los paquetes directamente a su CoA utilizando para ellos mensajes de Binding Update.

En la figura 6-1 se muestra el esquema de movilidad en IPv6:

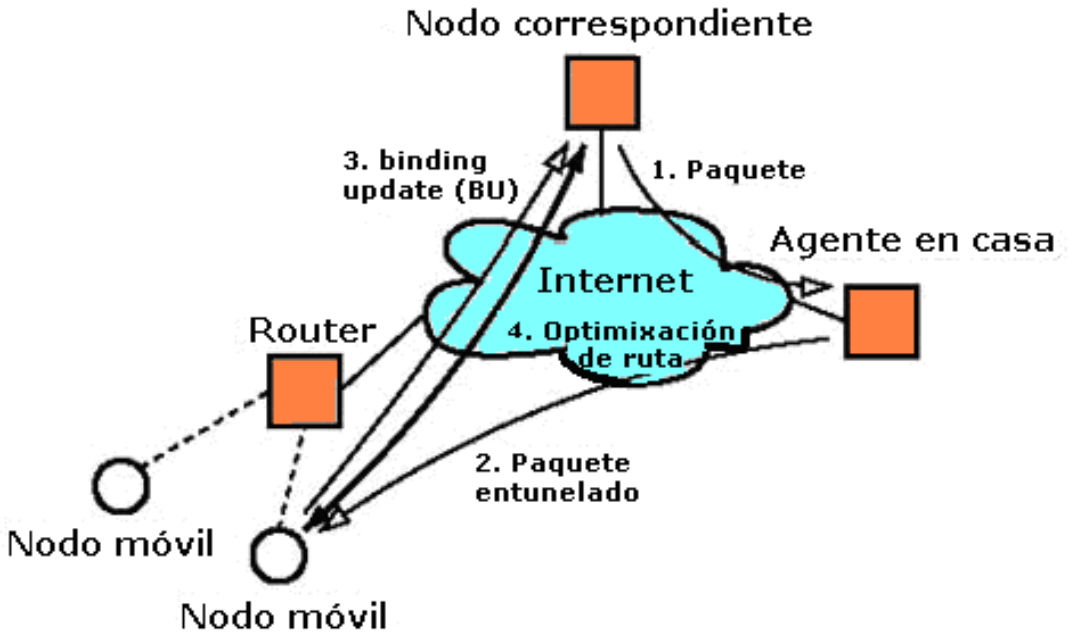



**Fig. 6-1. Movilidad IPv6.**

## 6.2. CABECERAS ADICIONALES.

Para conseguir toda esta funcionalidad añadida, Mobile IPv6 aprovecha las cabeceras de opción de destino. Esto permite enviar información de señalización en el mismo paquete de datos. Los nuevos tipos de opciones de destino creadas para soportar la movilidad son:

- **Home Address Option:** Indica cual es la dirección 'de casa' del nodo móvil cuando éste se encuentra fuera de su red origen.

- **Binding Update Option:** Que sirve para crear, actualizar y eliminar entrada de las asociaciones que se mantienen entre MN y CoA. Un paquete con esta opción hará que se produzca una asociación en el CN o en el HA entre la dirección origen del paquete y la dirección contenida en el campo de Home Address Option.

- **Binding Acknowledgement (BA) Option:** Es enviada por el HA y por el CN como respuesta a los BU enviados por el nodo móvil.

- **Binding Request (BR) Option:** Enviada por el CN para solicitar al nodo móvil refrescar su entrada en la lista de asociaciones actual del MN.

## 6.3. MECANISMO DE SEGURIDAD EN MOBILE IPV6.

Tanto los Binding Updates como los Binding Acknowledgements provocan un cambio de estado en los nodos, por los que deben de ser autenticados.

Mobile IPv6 utiliza autenticación de cabecera (Authentication Headers, AH) para evitar cualquier ataque.

Sin embargo, la autenticación no es el único problema. La autorización, es decir, que CN puede alterar qué asociaciones en la tabla de un MN (que afecta las tablas de enrutamiento). Una posible forma de solventar esto es utilizar IKE (Internet Key Exchange) junto a DNSSEC, asumiendo que tanto el nodo móvil como el CN utilizan la misma infraestructura de llave pública.

# CAPITULO VII

# CAPITULO VII: SEGURIDAD EN EL PROTOCOLO IPv6

Desde el repaso de la arquitectura IPv6, se podrá recordar que tanto el encabezado de extensión Authentification (AH) como Encryption (ESP) han sido definidos y son requeridos para una implementación completa de IPv6. Los encabezados Authentification y Encryption son parte del trabajo en curso en IP Security (Ipsec), que es direccionar aplicaciones para IPv4 e IPv6. Un archivo de los estándares Ipsec está disponible desde el Virtual Private Networking Consortium.

Las funciones de autentificación y cifrado (encryption) han sido separadas de tal manera que las implementaciones individuales pueden usar una o ambas de las funciones como sean necesitadas por las aplicaciones de capa más alta. Cifrado, por ejemplo, puede ser restringida para regulación gubernamental; así, solo la autentificación está implementada en algunos casos.

## 7.1. ARQUITECTURA DE SEGURIDAD IP (IPSEC)

La meta de IP Security (Ipsec) es proveer seguridad basada en criptografía, interoperable para IPv4 e IPv6. Como estas funciones de seguridad son ofrecidas en la capa IP, la protección para tanto IP como cualquier capa más alta de protocolos es proveída. Ipsec habilita a un sistema seleccionar los protocolos de seguridad requeridos, determinar los algoritmos que serán usados para el servicio de seguridad, e implementar cualquier clave criptográfica que sea requerida para proveer estos servicios. Ipsec puede ser usado para proteger los caminos de comunicación entre 2 hosts, entre 2 gateways de seguridad o entre un host y un gateway de seguridad.

La arquitectura de seguridad para IPv6 está definida en RFC 2401. Este documento incluye las siguientes definiciones base para varios sistemas y procesos:

- **Control de Acceso:** El proceso de prevenir acceso no autorizado a un recurso de red.

- **Autentificación:** La verificación de la identidad de la fuente reclamada de los datos (también conocido como autentificación del origen de los datos), más la propiedad que un paquete IP individual no ha sido modificado (integridad sin conexión).

- **Integridad:** La propiedad de asegurar que los datos son transmitidos desde una fuente o destino sin modificación sin detectar. Integridad sin conexión es un servicio que detecta la modificación de un paquete IP individual, sin importar el orden del paquete en un stream de datos. Integridad anti-replay (o integridad de secuencial parcial) detecta la llegada de paquetes IP duplicados dentro de una ventana.

- **Confidencialidad:** La protección de los datos de acceso no autorizado.

- **Cifrado:** Un mecanismo para transformar los datos desde una forma inteligente (plaintext) a una forma no inteligente (ciphertext), suministrando así confidencialidad.

- **Índice de Parámetros de Seguridad (SPI):** Un valor de 32 bits que es usado para distinguir entre diferentes Asociaciones de Seguridad (SAs) terminando en el mismo destino y usando el mismo protocolo IPSec.

- **Asociación de Seguridad (SA):** Una simple (unidireccional) conexión lógica, creada para propósitos de seguridad. Tanto AH como ESP hacen uso de SAs. La SA es una simple conexión lógica (de una vía) que provee servicios de seguridad a los AH o ESP pero no a ambos. Así, si tanto un AH como un ESP se les aplica el mismo stream de tráfico, 2 SA debe ser asignadas. Además, sesiones de comunicaciones bidireccionales, autentificadas entre 2 hosts tendrán 2 SA en uso (uno en cada dirección). La SA puede incluir: el algoritmo de autentificación, el algoritmo de cifrado, tiempo de vida de la clave, o tiempo en que la clave debe ser cambiada, y así. Dos tipos de SA son definidos: modo de transporte y modo túnel.

- **Gateway de Seguridad:** Un sistema que actúa como un sistema intermediario entre 2 redes. Los hosts o redes en el lado externo del gateway de seguridad son vistos como sistemas no confiables (o menos confiables), mientras que los hosts o redes en el lado interno son vistos como sistemas confiables (o más confiables).

- **Análisis de Tráfico:** El análisis del flujo de tráfico en la red para el propósito de deducir información que es útil para un adversario. Ejemplos de este tipo de información son la frecuencia de transmisión, las identidades de las partes que conversan, tamaño de los paquetes, identificadores de flujos usados, y así.

- **Subred Confiable:** Una red que contiene hosts y routers que se confían entre sí para no comprometerse en ataques activos o pasivos, y que

confían que el canal de comunicación subyacente (ejemplo: un Ethernet) no está siendo atacado.

- **Asociación de Seguridad en Modo de Transporte:** Una SA entre 2 hosts, primariamente proveyendo seguridad para los protocolos de capa más alta.

- **Asociación de Seguridad en Modo de Túnel:** Una SA aplicada a un túnel de IP, primariamente proveyendo seguridad para un paquete en el túnel.

Las siguientes secciones discuten las varias SA que son posibles, más la manera en que AH y ESP son implementadas dentro de estas SA.

## 7.2. ASOCIACIONES DE SEGURIDAD

La Asociación de Seguridad (SA) es una conexión lógica simple (o de una vía) que provee servicios de seguridad al tráfico que está siendo cargado sobre esa conexión. Estos servicios de SA pueden ser proveídos a AH o ESP pero no a ambos. Si se desean un AH y un ESP, dos SA son requeridos.

Dos tipos de SA son definidos: modo de transporte y modo de túnel. El SA en modo de transporte existe entre 2 hosts. Para el modo de transporte, el encabezado de protocolo de seguridad (AH o ESP) aparecería después del encabezado IP y otros encabezado de extensión opcionales, pero pueden aparecer antes o después del encabezado de destino, y antes de cualquier encabezado de protocolo de capa más alta como UDP o TCP. Cuando AH es empleado en modo de transporte, la seguridad es proveída para las porciones del encabezado IP y protocolos de capa más alta. Cuando ESP es empleado en modo de transporte, la seguridad es proveída para solo los protocolos de capa más alta.

En modo de túnel, la SA es aplicada al túnel. Donde un extremo del túnel es un gateway de seguridad, el modo de túnel debe ser usado. Si los dos extremos del túnel son hosts, entonces el modo de túnel o de transporte puede ser usado.

Para el modo de túnel, hay 2 encabezados IP: un encabezado externo que especifica el destino para el proceso Ipsec, y un encabezado interno que especifica el destino del paquete. Cuando AH es empleado en modo de túnel, la seguridad es proveída por porciones del encabezado externo IP más todo el paquete de túnel interno. Cuando ESP es empleado en modo de túnel, la seguridad es proveída solo para el paquete de túnel interno.

Una asociación de seguridad individual usa solo un protocolo de seguridad:

AH o ESP. Si la política de seguridad dicta habilidades que no son ejecutables con un solo protocolo de seguridad, múltiples SAs pueden ser usadas para esta implementación. El término paquete de asociación de seguridad es aplicado a esa condición. Las asociaciones de seguridad pueden ser combinadas en paquetes en 2 formas: un transporte adyacente o tunneling iterado. Con un transporte adyacente, más de un protocolo de seguridad es aplicado al mismo paquete IPv6, sin usar tunneling. Múltiples niveles de protocolos de seguridad son implementados a través de tunneling, con cada uno de estos túneles terminando posiblemente en un endpoint. Con el modo de transporte, si tanto AH como ESP son usados, AH debe aparecer como el primer encabezado después de IPv6, seguido por ESP. Con esta secuencia, la autentificación es así aplicada a la salida cifrada de ESP. Con el modo de túnel, órdenes diferentes de AH y ESP son posibles, dependiendo de los requerimientos de seguridad.

## 7.3. AUTENTIFICACIÓN

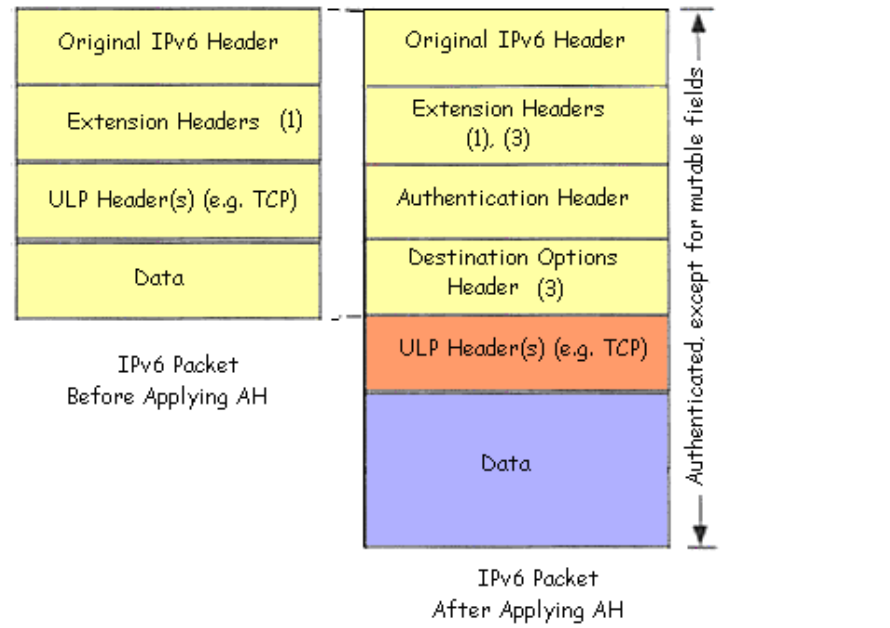
El Authentification Header (AH) provee integridad sin conexión, autentificación del origen de los datos y un servicio anti-replay opcional. AH está definido en RFC 2402. AH puede ser implementado en dos formas: modo de transporte (entre hosts) y modo de túnel (entre hosts y gateways de seguridad, o entre 2 hosts). AH es un protocolo apropiado para implementar cuando la confidencialidad no es requerida, o no es permitida (por regulaciones gubernamentales, por ejemplo).

Nótese que tanto ESP como AH pueden proveer autentificación. La diferencia clave entre los servicios de autentificación proveídos por los 2 protocolos es el grado de cobertura. ESP no protege ningún campo del encabezado IPv6 a menos que esos campos estén encapsulados por ESP. En contraste, AH puede tener un rango de cobertura más amplia.

En modo de transporte, AH está considerado una carga útil de extremo a extremo, así que debe ser colocado después de los encabezado hop-by-hop, routing y fragmentation. El encabezado (o los encabezados) Destination Options puede ser colocado antes o después de AH, como lo requiera la implementación específica.

El modo de túnel contiene tanto un paquete interno IPv6 (para el destino) como un paquete externo IPv6, que puede ser enviado a un gateway de seguridad intermedio. En modo de túnel, AH protege el paquete interno IP completo, incluyendo el encabezado del paquete interno IPv6.

En la figura 7-1 se muestra el Algoritmo de Autentificación:




Notes:
(1) If present
(2) Hop- Hop, Destination Options, Routing, Fragmentation headers, if present
(3)The Destinations Options header,if present, could be before AH, afterAH,or both

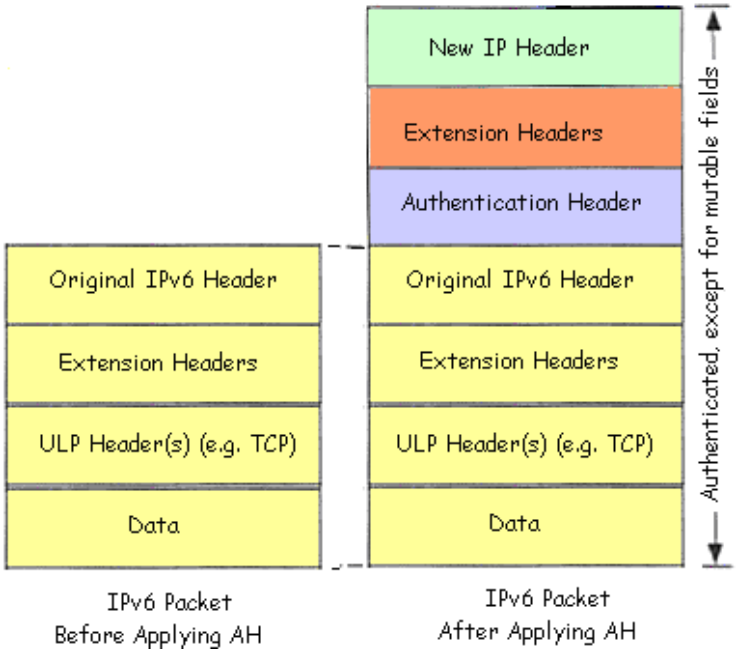



**Fig. 7-1. Autentificación.**

## 7.4. ENCRIPTACIÓN

Encapsulated Security Payload (ESP) provee confidencialidad (cifrado), autentificación del origen de los datos, integridad sin conexión, servicio anti- replay y confidencialidad de flujo de tráfico limitado (guardando contra análisis de tráfico). Tanto AH como ESP pueden ser usados para control de acceso, basado en los flujos de tráfico y distribución de claves en uso. El alcance de la autentificación ofrecido por ESP no es tan amplio como el proveído por AH.

En modo de transporte, ESP es considerado una carga útil de extremo a extremo, así que debe ser colocado después de los encabezado hop-by-hop, routing y fragmentation. El encabezado (o los encabezados) Destination Options pueden ser colocado antes o después de ESP. Sin embargo, como ESP protege solo los campos que van después del encabezado ESP, colocar el encabezado Destination Options después de ESP es deseable.

En la figura 7-2 se muestra el diagrama de Encriptación:

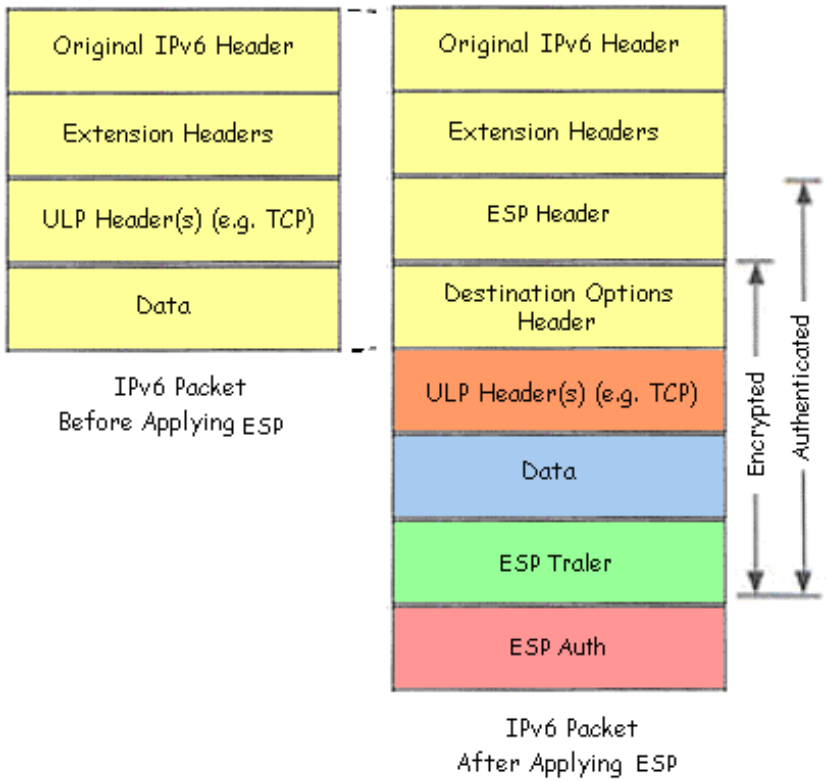



**Fig. 7-2. Encriptación.**

El modo túnel contiene tanto un paquete interno IPv6, para el destino, como un paquete externo IPv6, que puede ser enviado a un gateway de seguridad intermedio. En modo de túnel, ESP protege el paquete interno IP completo, incluyendo en encabezado del paquete interno IPv6.

En la figura 7-3 se muestra el diagrama de Encriptación Modo Túnel:

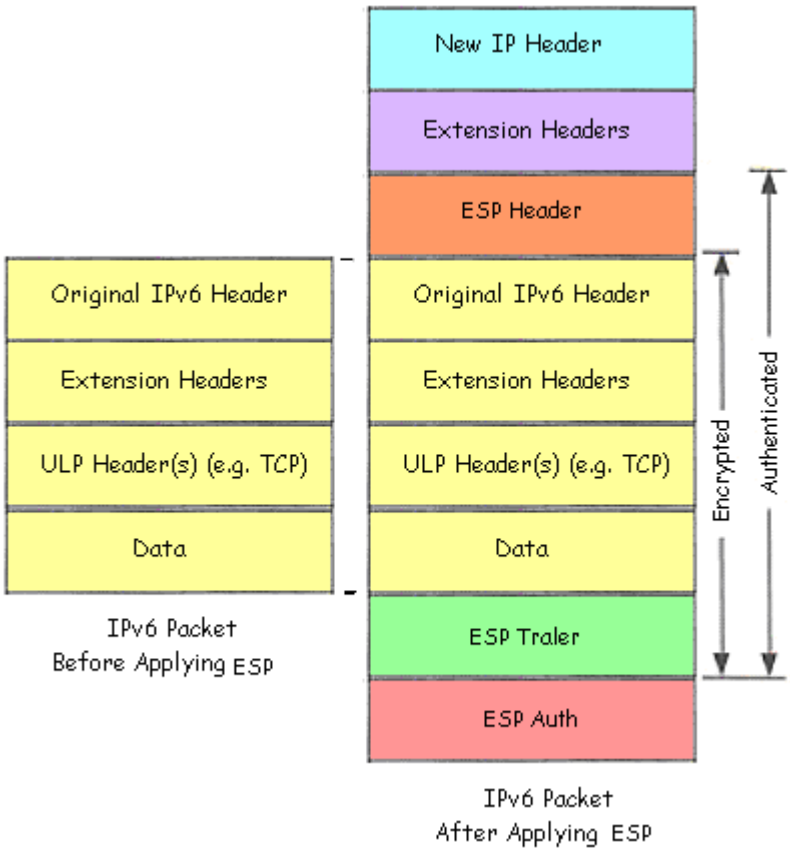



**Fig. 7-3. Encriptación Modo Túnel.**

Como se detalló en RFC 2406, Sección 5 (Conformance Requirements), una implementación obediente de ESP debe soportar los siguientes algoritmos mandados a implementar: HMAC con MD5 (descrito en RFC 2403), HMAC con SHA-1 (descrito en RFC 2404), DES en modo CBC (descrito en RFC 2405), el algoritmo NULL Authentification y el algoritmo NULL Encryption. Una referencia excelente sobre estos documentos varios es RFC 2411, el “IP Security Document Roadmap”.

# CAPITULO VIII

# CAPITULO VIII: INTEROPERABILIDAD

Puesto que Internet no va a amanecer un día utilizando de repente IPv6 en vez de IPv4, se han debido desarrollar una serie de métodos que permitan la convivencia y comunicación entre nodos, sea cual sea su versión de protocolo IP. Como se verá a continuación, se han desarrollado unos cuantos métodos de implementación, cada uno de ellos con sus ventajas e inconvenientes, pero sobretodo pensando en un principio para cada caso de migración distinto.

No utilizar un mecanismo de los aquí descritos u otro no tiene mucho sentido dada la pequeña cantidad de servicios que se están ofreciendo bajo la Internet utilizando el protocolo IPv6 actual. Como ejemplo está el de los servicios que se están ofreciendo bajo la Internet, que no llegarán al 1% comparado con lo que existe bajo IPv4.

Los desarrolladores de IPv6 reconocieron que no todos los sistemas se actualizarían desde IPv4 hacia IPv6 en el futuro inmediato, y algunos no se actualizarían por año. Para mayor complicación muchos de los sistemas de Internet son heterogéneos, con varios router, hosts, y son manufacturados por distintos vendedores. Si algo, como un multivendedor de sistema, fuera actualizado de una vez, la capacidad de IPv6 sería requerida en todos los elementos individuales antes de que el proyecto se realice.

Dado los contratiempos anteriores, se hace necesario desarrollar estrategia para la coexistencia de IPv4 e IPv6 hasta que llegue el momento en que IPv6 se convierta en la opción preferida.

Los siguientes términos están relacionados con nodo y están descritos para su uso en la arquitectura de transición definida en el RFC 1933:

- **Nodo IPv4-only:** Un host ó Router que implemente solamente IPv4 y que no entienda IPv6. La base IPv4 hosts y router existente antes de que empezara la transición.

- **Nodo IPv6/IPv4:** Es un host ó router que implemente tanto IPv4 como IPv6.

- **Nodo IPv6-only:** Es un host ó router que implemente IPv6 y que no implemente IPv4.

- **Nodo IPv6:** Cualquier host o router que implemente IPv6. IPv6/IPv4 y IPv6-only Node se pueden categorizar como IPv6 Node.

- **Nodo IPv4:** Cualquier host o router que implemente IPv4. IPv6/IPv4 y IPv4-only Node se pueden categorizar como IPv4 Node.

- **Direcciones IPv4 Compatible IPv6:** Una dirección IPv6 asignada a un nodo IPv6/IPv4, la cuál lleva el mayor orden de 96 Bits con el prefijo 0:0:0:0:0:0 y una dirección IPv4 en el menor orden de 32 Bits. Las direcciones compatibles IPv4 son usada por el mecanismo automático de tunneling.

- **Direcciones IPv6 Nativo:** Un host ó Router que implemente IPv6 sin necesidad de usar métodos de túneles. Éstas direcciones no llevan el prefijo 0:0:0:0:0:0.

## 8.1. TÚNELES.

Encapsular un paquete IP dentro de otro es un mecanismo conocido y se usa en la actualidad sobretodo para crear redes privadas virtuales. La utilidad que se le dará aquí es para enlazar nubes o islas IPv6 en una Internet basada prácticamente en su totalidad en IPv4; en la figura 8-1 se muestra el esquema.

Tenemos dos tipos básicos de túneles: estáticos y dinámicos. El 6bone actual está formado en su mayoría por túneles estáticos.

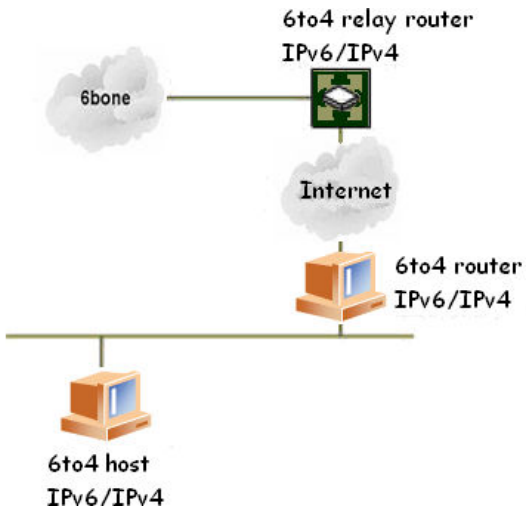



**Fig. 8-1. Túneles.**

El proceso de encapsulación esta ilustrado en la figura 8-2. Se puede notar que el resultado del datagramas IPv4 contiene entre el encabezado IPv4 y el encabezado IPv6, toda la información de la capa superior, por ejemplo los encabezado TCP, datos de aplicación, entre otros. El proceso inverso de desencapsulación, se encuentra ilustrado en la figura 8-3. En este caso, los encabezados IPv4 son removidos, dejando solamente los paquetes IPv6. Dentro del encabezado IPv4, el valor del campo de protocol tendría un valor de 41, identificando que es IPv6.

El proceso de túneles implica 3 pasos distintos: encapsulación, desencapsulación y administración de túnel. En el nodo encapsulado (o el punto de entrada del túnel), el encabezado IPv4 es creado y el paquete encapsulado para ser transmitido. En el nodo desencapsulación (o punto de salida del túnel), los encabezados IPv4 son removidos y el paquete IPv6 es procesado. Además, la encapsulación en el nodo puede mantener la información de configuración mientras los túneles están establecidos.

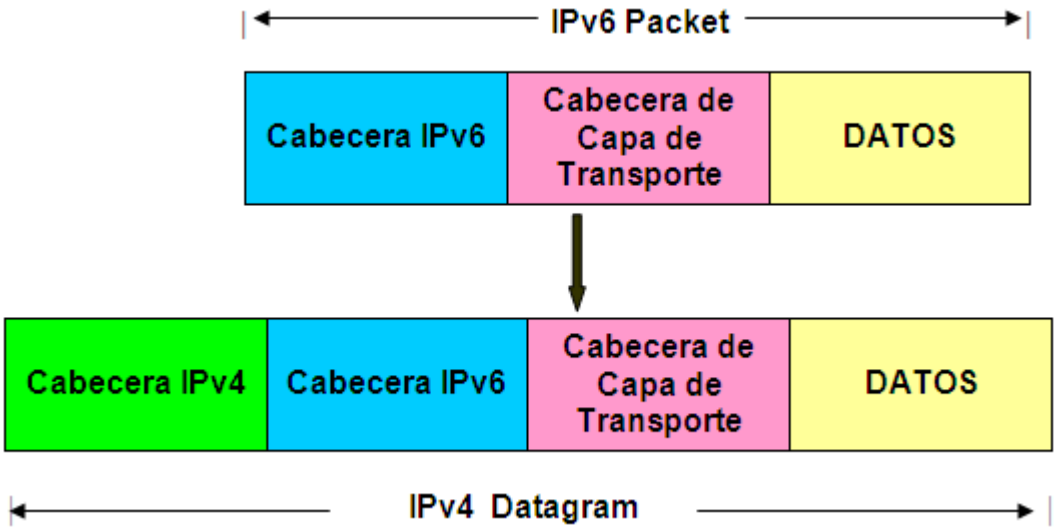



**Fig. 8-2. Proceso de Túneles (Encapsulado).**

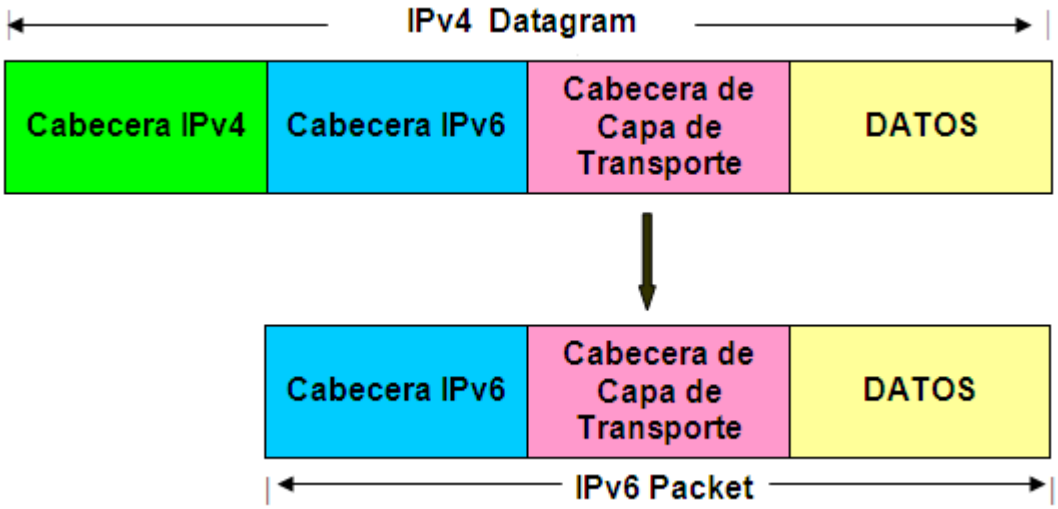



**Fig. 8-3. Proceso de Túneles (Desencapsulado).**

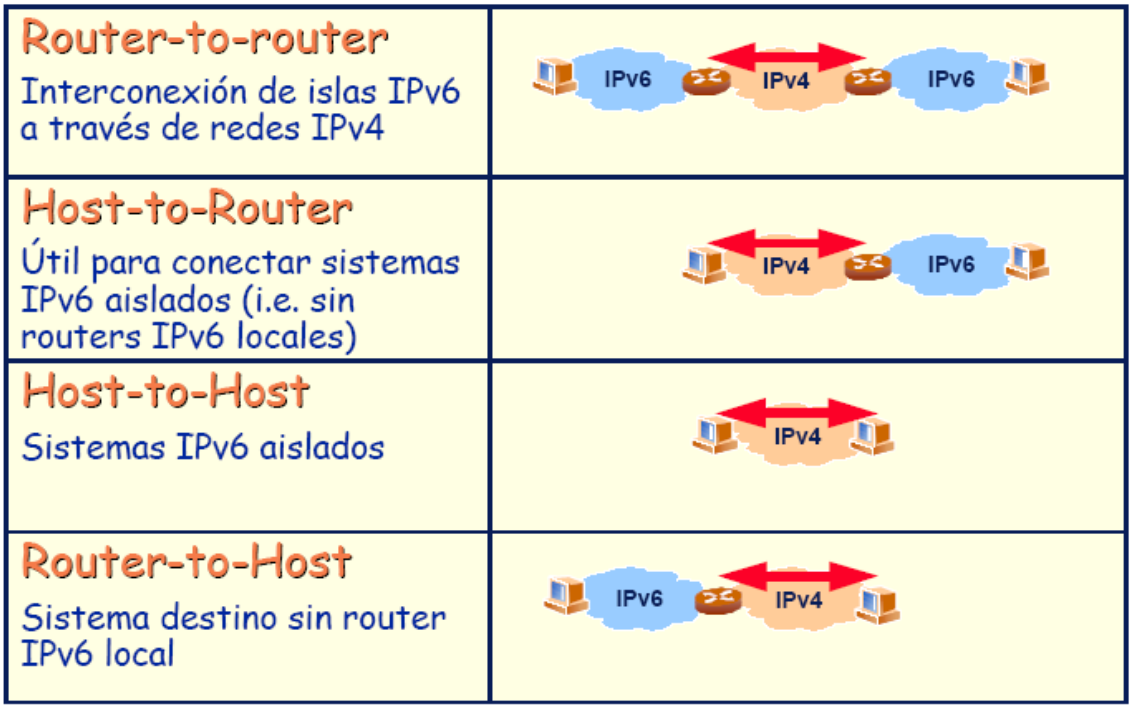



**Fig.8-4. Tipos de Túneles**

### 8.1.1. Túneles Estáticos.

Esta es la solución más sencilla si se quiere tener acceso tanto a IPv6 como a IPv4.

El caso más común será un host con IPv4 que desee tener acceso a la red IPv6 existente. Para ello se deberá crear un túnel con un router a través de IPv4 que tenga tanto acceso a IPv6 como a IPv4. Un caso un poco menos común para el usuario es el que se desee unir "islas" IPv6, o sea, unir redes IPv6, utilizando para ello la infraestructura de IPv4 existente.

Este método se está utilizando en la actualidad por parte de algunos proveedores de servicios para que cualquiera pueda tener acceso a la red IPv6.

Dentro de esta categoría podemos considerar también la de los servidores de túneles, que en estos momentos son interfaces web que permiten la creación de túneles bajo demanda a cualquier usuario.

### 8.1.2. 6 to 4

Este mecanismo se puede aplicar para comunicar redes IPv6 aisladas por medio de la red IPv4. El router extremo de la red IPV6 crea un túnel sobre IPv4 para alcanzar la otra red IPv6. Los extremos del túnel son identificados por el prefijo del sitio IPv6. Este prefijo consiste en 16 Bits fijos que indican que estamos utilizando la técnica 6to4 más 32 Bits que identifican al router externo del 'sitio'.

Un efecto secundario de 6to4 es que deriva automáticamente un prefijo /48 de una dirección IPv4. De esta forma, los 'sitios' pueden empezar a utilizar IPv6 sin solicitar nuevo espacio de direccionamiento a la autoridad competente.
La figura 8-5 muestra el esquema 6 to 4:

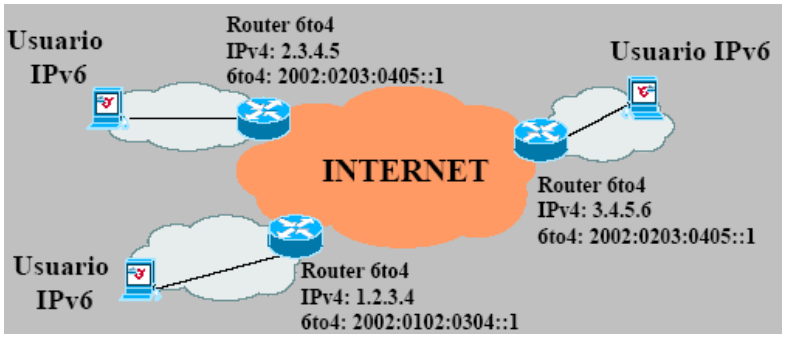



**Fig. 8-5. 6 to 4.**

### 8.1.3. 6 over 4

Puede que no se tenga una red de sitio homogénea en el aspecto de que todos los nodos puedan comunicarse entre si con la misma versión de protocolo IP. Con este método se podrán comunicar nodos IPv6 aislados dentro de nuestro 'sitio' con el resto de nodos IPv4. Esta técnica también se emplea en casos en los cuales el router IPv6 no tiene acceso o permiso para transmitir paquetes IPv6 sobre enlace. Para salvar este inconveniente se creará un enlace virtual utilizando un grupo multicast IPv4, mapeando las direcciones IPv6 sobre este grupo multicast.

La figura 8-6 muestra el esquema 6 over 4:

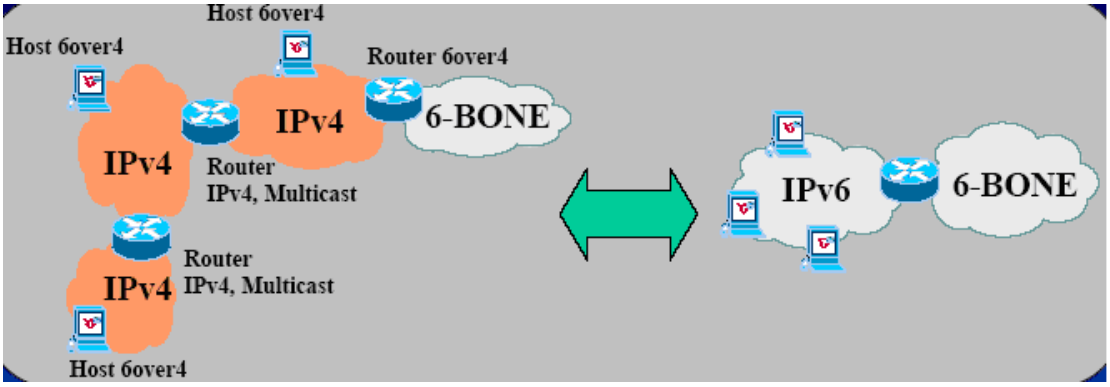



**Fig.8-6 6 over 4.**

### 8.1.4. Intra-Site Automatic Tunel Addressing Protocol (ISATAP)

Como su nombre indica, este método también está pensado para la comunicación entre nodos de un mismo 'sitio'. Tiene algunas ventajas respecto a 6 over 4, como que no necesita multicast IPv4 y que soluciona los problemas que se dan cuando una misma organización no tiene toda su red en un mismo lugar, como la baja escalabilidad en la agregación.

La técnica funciona empotrando la dirección IPv4 del nodo en el identificador EUI-64 del interfaz. Puesto que este método viene a solucionar los problemas de comunicación dentro de un 'sitio' las direcciones IPv4 no tienen porqué ser globales. Esto significa que aunque exista NAT, el mecanismo seguirá funcionando correctamente.

## 8.2. COMUNICACIÓN ENTRE NODOS

Una vez se tienen unidas varias islas IPv6, el problema que se plantea es que todos los nodos puedan acceder a la Internet IPv6 como a la IPv4. La solución la a consistir en o bien a nivel de aplicación, transformando la capa de enlace o asignando temporalmente direcciones IPv4 a nodos IPv6.

### 8.2.1. Doble Pila

En este modelo, todos los nodos presentes en la red tienen doble pila. De esta forma, la comunicación con los nodos IPv4 se hace con la pila de IPv4 y con IPv6 se hace con la pila de IPv6.

Todos los nodos en la red tienen que tener doble pila. Esto en una red de gran tamaño puede llegar a ser un problema serio a la hora de hacer la migración.

### 8.2.2. Stateless IP/ICMP Translation Algorithm (SIIT)

Este algoritmo traduce entre encabezados de IPv4 e IPv6 (Incluyendo los encabezados ICMP). Este nuevo algoritmo puede usarse como parte de una solución que permite a ordenadores con IPv6 comunicarse con ordenadores con IPv4.

El protocolo SIIT permite traducir entre IPv6 e IPv4. Esta traducción queda limitada a la cabecera IP. Como su propio nombre dice, no se realiza un control de estado, por lo que la traducción se debe realizar para cada paquete.

### 8.2.3. Network Address Translation – Protocol Translation (NAT-PT)

Enrutamiento transparente, para comunicar host que tienen IPv6 únicamente con host que tienen IPv4 únicamente.

En caso de que se tenga un nodo o bien con IPv6 o bien con IPv4 de forma exclusiva, ésta puede ser una buena solución. La comunicación se realiza a través de un dispositivo específico (un router que soporte NAT-PT) y que soporta el control de estado de las conexiones. Este método necesita también cambios a nivel de aplicación para controlar las peticiones de resolución de nombre en el DNS.

### 8.2.4. Bump in the Snack (BIS)

Si se piensa en el método de NAT-PT a nivel particular de cada host, se llegará a tener una idea de en qué consiste este mecanismo, que se utilizará en caso de que las aplicaciones que utilicen los nodos no soporten IPv6.

Añadiendo tres módulos (una extensión para la resolución de nombres, un maleador de direcciones y un traductor) entre el nivel de aplicación y el de red se consigue un acceso transparente a nodos IPv6.

La idea es la siguiente: cuando una aplicación exclusiva IPv4 necesita comunicarse con un nodo IPv6, la dirección IPv6 de ese nodo se mapea a una dirección IPv4. Los paquetes IPv4 generados se transforman en paquetes IPv6 utilizando SIIT.

### 8.2.5. SOCKS64

SOCKS es una Puerta de Enlace (Gateway) entre dos redes que permite que ciertas aplicaciones se comuniquen con sus contrapartes en la otra red, en este caso desde una red IPv4 a una IPv6 o viceversa.

Esta solución puede llegar a ser la ideal en caso de que el 'sitio' esté utilizando ya SOCKS. Con un gateway de tipo SOCKS64 se puede permitir conectar a los clientes tanto a nodos IPv4 como IPv6, sin los típicos problemas asociados a los túneles (Fragmentación y Límite de Saltos).

La comunicación a través de un servidor SOCKS es dependiente de la aplicación, esto quiere decir que si alguna aplicación no tiene soporte para SOCKS no se va a poder comunicar con su contraparte. Además es un solo punto de falla.

# CAPITULO IX

# CAPITULO IX: POLÍTICA DE ASIGNACIÓN Y DELEGACIÓN DE DIRECCIÓN IPv6

Estas políticas fueron un desarrollo conjunto por las comunidades APNIC, ARIN y RIPE.

## 9.1. DESCRIPCIÓN

Se describen las políticas para la asignación y delegación del espacio de dirección globalmente único de Internet Protocol Versión 6 (IPv6). Las políticas descritas en este artículo están pensadas a ser adoptadas en cada registro. Sin embargo, la adopción de estas políticas no imposibilita variaciones locales en cada región o área.

Los RFC2373 y RFC2373bis designan 2000::/3 a ser el único espacio de dirección unicast global que IANA puede asignar a los RIR. De acuerdo con RFC2928, RFC2373bis, IAB-Request, IANA ha asignado rangos iniciales de espacio de dirección IPv6 unicast global desde el bloque de dirección 2001::/16 a los RIR existentes. Este documento concierne a las asignaciones sub- secuentes del espacio de dirección unicast 2000::/3, por el que los RIRs formulan las políticas de asignación. Porque a los sitios finales se les dará /48 asignaciones según describe RFC3177, el énfasis particular de este articulo está en las políticas relativas a los bits de 2000::/3 a la izquierda del limite /48.

Sin embargo, como algunos sitios finales recibirán asignaciones /64 y /128, todos los bits a la izquierda de /64 están en el alcance.

Esta política está considerada a ser una política interina. Será revisada en el futuro, sujeto a una experiencia más grande en la administración de IPv6.

## 9.2. DEFINICIONES

Los siguientes términos y sus definiciones son de particular importancia para el entendimiento de las metas, ambiente y políticas descritas en este artículo.

La responsabilidad del manejo de los espacios de dirección es distribuida globalmente de acuerdo a la estructura jerárquica mostrada en la figura 9-1:

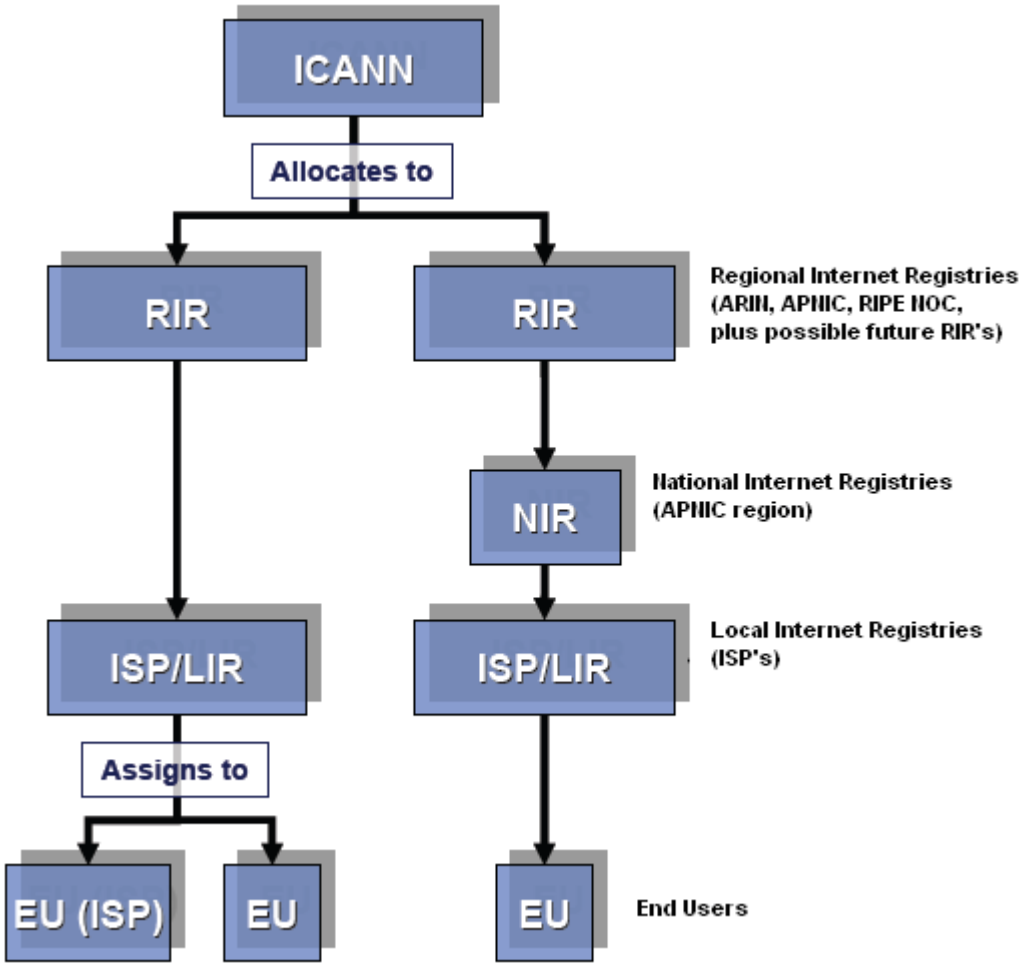



**Fig. 9-1. Estructura Jerárquica De Asignación De Direcciones.**

- ✓ **Internet Registry (IR):** Registro de Internet (Internet Registry, IR) es una organización que es responsable de distribuir espacios de dirección IP a sus miembros o clientes y de registrar estas distribuciones. Los IR son clasificados de acuerdo a su función primaria y alcance territorial dentro de la estructura jerárquica vista en la figura.

- ✓ **Regional Internet Registry (RIR):** Los RIR están establecidos y autorizados por las respectivas comunidades regionales, y reconocidas por el IANA para servir y representar grandes regiones geográficas. El rol

primario de los RIR es manejar y distribuir el espacio de dirección de Internet público en sus respectivas regiones.

- ✓ **National Internet Registry (NIR):** Un registro de Internet Nacional asigna primariamente el espacio de dirección a sus miembros y constituyentes, que son generalmente LIRs organizados a un nivel nacional. Los NIR existen mayormente en la región Asia-Pacifico.

- ✓ **Local Internet Registry (LIR):** Un registro de Internet Local (LIR) es un IR que asigna primariamente espacio de dirección a los usuarios de los servicios de red que provee. Los LIR son generalmente ISPs, cuyos clientes son primariamente usuarios finales u otros posibles ISPs.

- ✓ **Asignar:** Significa distribuir espacio de dirección a los IR para el propósito de distribución sub-secuente de ellos.

- ✓ **Delegar:** Significa delegar espacio de dirección a un ISP o usuario final, para uso especifico dentro de la infraestructura de Internet que ellos operan. Las delegaciones deben ser hechas solo para propósitos específicos documentados por organizaciones especificas y nos sub-delegadas a otras partes.

- ✓ **Utilización:** No como en IPv4, IPv6 es generalmente delegado a sitios finales en cantidades fijas (/48). El uso actual de direcciones dentro de cada asignación será muy bajo, cuando se compara con las asignaciones de IPv4. En IPv6, 'utilización' es solo medido en término de bits a la izquierda del limite /48. En otras palabras, la utilización se refiere a la asignación de /48s a sitios finales, y no el número de direcciones asignadas dentro de /48s individuales a esos sitios finales. A través de este documento, el término utilización se refiere a la asignación de /48s a sitios finales y no al número de direcciones asignadas dentro de /48s individuales a esos sitios finales.

- ✓ **HD-Ratio:** El promedio HD, es una forma de medir la eficiencia de la asignación de direcciones [RFC 3194]. Es una adaptación de H-Ratio originalmente definido en [RFC 1715] y es expresado como sigue:

$$HD = \frac{\text{Log (number of allocated objects)}}{\text{Log (maximum number of allocatable objects)}}$$

Donde (en el caso de dicho articulo) los objetos son direcciones de site IPv6 (/48s) delegados desde un prefijo IPv6 de un tamaño dado.

- ✓ **Sitio Final:** Un sitio final es definido como un usuario final (suscriptor) que tiene una relación de negocios con un proveedor de servicio que envuelve:

    - Que ese proveedor de servicio delegue espacio de dirección a ese usuario final.
    - Que ese proveedor de servicio provea servicio de tránsito para el usuario final a otros sitios.
    - Que ese proveedor de servicio cargue el tráfico del usuario final.
    - Que ese proveedor de servicio haga publicidad de un prefijo de ruteo agregado que contenga la asignación del usuario final.

## 9.3. POLÍTICAS PARA ASIGNACIONES Y DELEGACIONES

Para calificar para una asignación inicial de espacio de dirección IPv6, una organización debe:

1. Ser un LIR.
2. No ser un sitio final.
3. Planear proveer conectividad IPv6 a organizaciones a quienes le asignará /48s mediante publicidad.
4. Tener un plan para hacer al menos 200 asignaciones /48 a otras organizaciones dentro de 2 años.

Las organizaciones que cumplan los criterios de asignación inicial son elegibles para recibir una asignación mínima de /32.

Las organizaciones pueden calificar para una asignación inicial más grande de /32 mediante documentación sometida que justifique razonablemente la solicitud. Si es así, el tamaño de asignación será basado en el número de usuarios existentes y el grado de la infraestructura de la organización.

Las organizaciones que tengan una asignación IPv6 existente pueden recibir asignaciones sub-secuentes de acuerdo con las políticas.

La asignación sub-secuente será proveída cuando una organización (ISP/LIR) satisfaga la evaluación limite de la utilización de pasadas direcciones en términos del número de sites en unidades de asignación /48. El HD-Ratio [RFC 3194] es usado para determinar la utilización que justifica las asignaciones adicionales como se describe debajo.

El valor del HD-Ratio de 0.8 es adoptado como se indica una utilización de espacio de dirección aceptable para justificar la asignación de espacio de dirección adicional.

Cuando una organización ha cumplido una utilización aceptable para su espacio de dirección asignado, es inmediatamente elegible para obtener una asignación adicional que resulta en el doble del espacio de dirección asignado a éste. Donde sea posible, la asignación será hecha desde un bloque de dirección adyacente, significando que su asignación existente es extendida por 1 bit hacia la izquierda.

Si una organización necesita más espacio de dirección, ésta debe proveer documentación justificando sus requerimientos por un período de 2 años. La asignación hecha será basada en este requerimiento.

No hay una política específica para que una organización (LIR) asigne espacio de dirección a ISPs subordinados. Cada organización LIR puede desarrollar su propia política para ISPs subordinados para una utilización optima del bloque de dirección total asignado al LIR. Sin embargo, todas las asignaciones /48 a sitios finales están requeridas a ser registradas por el LIR o sus IPSs subordinados de forma tal que el RIR/NIR pueda evaluar propiamente el HD-Ratio cuando una asignación subsecuente se hace necesaria.

Los LIR deben hacer asignaciones IPv6 de acuerdo con las siguientes provisiones.

Las asignaciones serán hechas de acuerdo con las guías existentes [RFC 3177, RIRs-on-48], que están resumidas aquí como:

- /48 en el caso general, excepto por suscriptores muy grandes.

- /64 cuando es conocido que una y solo una subred se necesita por diseño.

- /128 cuando absolutamente sabido que uno y solo un dispositivo está conectando.

A los RIR/NIR no le es referida que tamaño de dirección un LIR/ISP asigne. Por consiguiente, los RIR/NIR no solicitarán la información detallada en redes de usuario IPv6 como hacían en IPv4, excepto por algunos casos que lo ameriten y para los propósitos de medir la utilización como se definió anteriormente.

Cuando un sitio final siempre requiere un bloque adicional de dirección /48, debe requerir la asignación con documentación o materiales que justifiquen la solicitud. Solicitudes para múltiples o adicionales /48s serán procesadas y revisada (por ejemplo, evaluación de justificación) en el nivel RIR/NIR.

Una organización (ISP/LIR) puede asignar un /48 por PoP como infraestructura de servicio de un operador de servicio IPv6. Cada asignación a un PoP está visto como una asignación sin importar el número de usuarios que usan el PoP está visto como una asignación sin importar el número de usuarios que usan el PoP. Una asignación separada puede ser obtenida para las operaciones In- House del Operador.

## 9.4. REGISTRO

Cuando una organización manteniendo una asignación de dirección IPv6 hace asignaciones de dirección, ésta debe registrar la información de la asignación en una base de datos, accesible por los RIR como apropiado (Información registrada por un RIR/NIR puede ser reemplazada por una base de datos distribuida para registrar información de manejo de dirección en un futuro). La información es registrada en unidades de redes /48 asignadas. Cuando más de un /48 es asignado a una organización, la organización de la asignación es responsable de asegurar que el espacio de dirección está registrado en una base de datos RIR/NIR.

Los RIR/NIR usarán datos registrados para calcular el HD-Ratio al tiempo de la aplicación para asignación subsiguiente y para chequear los cambios en asignaciones en el tiempo.

Los IR mantendrá sistemas y prácticas que protejan la seguridad del personal y la información comercial que es usada en la evaluación de la solicitud, pero que no es requerida para registro público.

Cuando un RIR/NIR delega espacio de dirección IPv6 a una organización, también delega la responsabilidad de manejar la zona de operaciones de búsqueda en reverso que corresponde al espacio de dirección IPv6 asignado.

Cada organización debe manejar apropiadamente su zona de operaciones de búsqueda en reverso. Cuando se hace una asignación de dirección, la organización debe delegar a una organización cesionaria, bajo solicitud, la responsabilidad de manejar la zona de operaciones de búsqueda que corresponde a esa dirección asignada.

Las organizaciones que reciben asignaciones IPv6 /35 bajo la política anterior de dirección IPv6 [RIRv6 -Policies] tiene inmediatamente el derecho de tener su asignación expandida a un bloque de dirección /32, sin proveer justificación, mientras satisfagan los criterios. El bloque de dirección /32 contendrá el bloque de dirección más pequeño (uno o múltiples bloques de direcciones /35 en muchos casos) que ya fue reservado por el RIR para una asignación sub- secuente a la organización. Solicitudes para espacio adicionales más allá del tamaño mínimo /32 serán evaluadas.

# CAPITULO X

## CONCLUSIONES

- ✓ Debemos tener en cuenta principalmente que IP versión 6 no nace solo para solventar el problema del direccionamiento. IP versión 6 nos ayuda también a mejorar temas como el de la calidad del servicio, la seguridad, la movilidad y la velocidad de la red.

- ✓ Con el nuevo protocolo IP versión 6 Internet se convertirá en una red más rápida, más segura y fiable para todos, permitiendo el trabajo de aplicaciones en tiempo real. La transición a IPv6 es un proceso largo, complejo y muy costoso, pero las aplicaciones marcaran el ritmo de la transición.

- ✓ Es importante tener presente que la transición no es la solución a todos los problemas. De hecho, algunas aplicaciones innovadoras necesitan IPv6 para su despliegue masivo. Desplegar mecanismos de transición a gran escala puede además implicar problemas de escalabilidad que podrían limitar enormemente el rendimiento de IPv6 en comparación una solución nativa.

- ✓ IP versión 6 tiene la gran ventaja de que es compatible con su anterior versión de 32 bits, lo que le permite coexistir en la misma red. Las implementaciones de este nuevo protocolo empiezan a estar disponibles, y gracias a su compatibilidad permiten a los administradores de redes y directores de sistemas ir realizando las mejoras necesarias en sus equipos de forma temporal, teniendo en cuenta sus posibilidades y sin importar el tiempo empleado.

- ✓ Este nuevo protocolo nos permite seguir trabajando con las direcciones de 32 bits de su antecesor de forma concurrente, de igual forma que con las actuales aplicaciones TCP/IP. De este modo se da tiempo a los programadores a que vayan adaptando sus aplicaciones de forma paulatina a este protocolo.

- ✓ Al tener en cuenta todos los problemas que debería solventar este protocolo, y considerando todas estas características ha resultado un protocolo de capa de red compacto y robusto. Por tanto la meta del IPv6 es la de conseguir una mayor rapidez y flexibilidad con bastante espacio de direcciones.

- ✓ Se retiraron todos los campos relacionados con la fragmentación, puesto que el IPv6 tiene un enfoque distinto frente a la fragmentación. Cuando una

estación manda un paquete de IPv6 demasiado grande, en lugar de fragmentarlo, el router que es capaz de reenviarlo devuelve un mensaje de error. Este mensaje indica a la estación que divida todos los paquetes antes de enviarlos a ese destino. Es más eficiente que la estación origen fragmente los paquetes y los mande ya con un tamaño correcto.

- ✓ La diferencia básica que tiene Ipv6 sobre Ipv4 es la referente a que las direcciones IP pasaron de 32 bits a 128 bits, esto permite soportar más niveles de direccionamiento jerárquico, un mayor número de nodos direccionables y la simplificación de autoconfiguración de las direcciones.

- ✓ IPv6 permite manejar múltiples direcciones por interfaz de dispositivo haciendo la ruta simple y eficiente. En el caso de Ipv4, las direcciones tienen muy poca o ninguna conexión con los caminos de enrutamiento, por lo tanto los enrutadores del mantener enormes tablas de caminos de enrutamiento mientras que en Ipv6 los enrutadores mantienen pequeñas tablas de prefijos que permiten que la fuente envié los paquetes al destino correcto.

# BIBLIOGRAFÍA

## LIBROS:


- ✓ Implementing IPv6 (Second Edition)
Miller, Mark A., P.E.
Editorial: M&T Books
Segunda Edición, 2000
Foster City, California

- ✓ Internet Routing Architectures (Second Edition)
Halabi, Sam
Editorial: Cisco Press
Segunda Edición, 2001
Indianápolis, IN

- ✓ Internetworking IPv6 with Cisco Routers
Gai, Silvano
Editorial: McGraw-Hill Computer Communications Series
1998

- ✓ Configuring IPv6 for Cisco IOS
Sam Brown, Neal Chen, Paul J. Fong, Robbie Harrell
Editorial: Syngress
2002

- ✓ Internet: Manual de Referencia
Harley Hahn, Rick Stout
Editorial: Osborne/McGraw-Hill
Primera Edición, 1995
Aravaca, Madrid


## INTERNET:


- ✓ http://www.IPv6forum.com/navbar/documents/6WIND-IPv6-answers- 2.0.pdf

- ✓ http://www.IPv6forum.com/navbar/papers/MobileIPv6_Whitepaper.pdf

- ✓ http://www.isoc.org/inet2000/cdproceedings/1c/1c_2.htm

- ✓ http://www.arin.net/policy/IPv6.html

- ✓ http://www.rfc-editor.org/index.html
- ✓ ftp://ftp.rfc-editor.org/in- notes/rfc2463.txt
- ✓ ftp://ftp.rfc-editor.org/in- notes/rfc2462.txt
- ✓ ftp://ftp.rfc-editor.org/in- notes/rfc2461.txt
- ✓ ftp://ftp.rfc-editor.org/in- notes/rfc2460.txt
- ✓ http://www.ietf.org/internet-drafts/draft- ietf-v6ops-3gpp-analysis-08.txt

# ANEXO 1: RFC's IPv6

| | DOCUMENTO | TITULO |
|---|---|---|
| **Especificaciones Básicas** | RFC2460 | Especificaciones del Protocolo Internet Versión 6 (IPv6) |
| | RFC2461 | Descubrimiento del Vecindario para IPv6 (ND) |
| | RFC2462 | Autoconfiguración de Direcciones "stateless" IPv6 |
| | RFC2463 | Protocolo de Mensajes de Control de Internet para IPv6 (ICMPv6) |
| | RFC1981 | Descubrimiento del MTU de la ruta para IPv6 |
| | RFC1809 | Uso del Campo "Etiqueta de Flujo" en IPv6 |
| **Direccionamiento** | RFC2373 | Arquitectura de Direccionamiento en IPv6 |
| | RFC1887 | Arquitectura para la Asignación de Direcciones Unicast IPv6 |
| | RFC2374 | Formato de Direcciones Unicast Agregables Globales |
| | RFC2450 | Propuesta de Normas de Asignación de TLA y NLA |
| **Routing** | RFC2080 | RIP para IPv6 |
| | RFC2081 | Aplicabilidad de RIPng para IPv6 |
| | RFC2283 | Extensiones Multiprotocolo para BGP-4 |
| | RFC2545 | Uso de las Extensiones Multiprotocolo de BGP-4 para Routing entre Dominios para IPv6 |
| | RFC2740 | OSPF para IPv6 |
| **DNS** | RFC1886 | Extensiones DNS para Soportar IPv6 |
| **IPv6 sobre…** | RFC2464 | Transmisión de Paquetes IPv6 sobre Redes Ethernet |
| | RFC2467 | Transmisión de Paquetes IPv6 sobre Redes FDDI |
| | RFC2470 | Transmisión de Paquetes IPv6 sobre Redes Token Ring |
| | RFC2472 | IPv6 sobre PPP |
| | RFC 2491 | IPv6 sobre Redes de Acceso Múltiple sin Broadcast |
| | RFC2492 | IPv6 sobre Redes ATM |
| **Seguridad** | RFC2401 | Arquitectura de Seguridad para IP |
| | RFC2402 | Cabecera de Autenticación IP |

| | | |
|---|---|---|
| | RFC2406 | Encriptación de Datos en IP (ESP) |
| | RFC2408 | Asociaciones de Seguridad y Protocolo de Gestación de Claves en Internet (ISAKMP) |
| **Multicast** | RFC2375 | Asignación de Direcciones Multicast |
| | RFC2710 | Descubrimiento de Nodos que desean recibir Multicast para IPv6 |
| | RFC2776 | Protocolo de Anunciación de Zonas de Ámbito Multicast (MZAP) |
| **Anycast** | RFC2526 | Direcciones de Subredes para Anycast en IPv6 |
| **Multi-Homing** | RFC2260 | Soporte Escalable de Multi-Homing para Conectividad Multi-Proveedor |
| | RFC2497 | Transmisión de Paquetes IPv6 sobre Redes ARCnet |
| **Transición** | RFC1933 | Mecanismos de Transición para Routers y Hosts IPv6 |
| | RFC2185 | Aspectos de Routing de la Transición IPv6 |
| | RFC2473 | Especificaciones Genéricas de Tunelización de Paquetes en IPv6 |
| | RFC2529 | Transmisión de IPv6 sobre Dominios IPv4 sin Túneles Explícitos |
| | RFC2765 | Algoritmo de Traslación Stateless IP/ICMP (SIIT) |
| | RFC2766 | Protocolo de Traslación - Traslación de Dirección de Red |
| | RFC2767 | Doble Pila en Hosts usando la Técnica "Bump-In-the-Stack" (BIS) |
| **API** | RFC2292/bis | Advanced Sockets API para IPv6 |
| | RFC2553/bis | Basic Socket API para IPv6 |
| **MIB** | RFC2452 | Base de Información de Gestión para IPv6: TCP |
| | RFC2454 | Base de Información de Gestión para IPv6: UDP |
| | RFC2465 | Base de Información de Gestión para IPv6: Conversaciones Textuales y Grupo General |
| | RFC2466 | Base de Información de Gestión para IPv6: ICMPv6 |

| | | |
|---|---|---|
| **Otros** | RFC1881 | Gestión de la Asignación de Direcciones IPv6 |
| | RFC1924 | Representación Compacta de Direcciones IPv6 |
| | RFC2147 | TCP y UDP sobre Jumbogramas IPv6 |
| | RFC2428 | Extensiones FTP para IPv6 y NAT |
| | RFC2471 | Plan de Asignación de Direcciones IPv6 para Pruebas |
| | RFC2474 | Definición del Campo de Servicios Diferenciados (DS) en Cabeceras IPv4 e IPv6 |
| | RFC2546 | Prácticas de Routing en 6Bone |
| | RFC2663 | Consideraciones y Terminología de IP NAT |
| | RFC2732 | Formato para la Representación literal de direcciones IPv6 en URL's |
| | RFC2772 | Guías de Routing en el Troncal 6Bone |
| | RFC27175 | Transparencia de Internet |